Accton
Making Partnership Work

VDSL Switch-VS4512
VDSL Switch-VS4512DC

Management Guide

Accton

Making Partnership Work

Management Guide

VDSL Switch-V4512

VDSL Switch supporting 12 VDSL lines, with 2 Slots for Optional 1000BASE-SX, 1000BASE-LX, 1000BASE-T or 1000BASE-X GBIC uplink modules

VDSL Switch-VS4512DC

VDSL Switch supporting 12 VDSL lines, with 2 Slots for Optional 1000BASE-SX, 1000BASE-LX, 1000BASE-T or 1000BASE-X GBIC uplink modules

Accton makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability, quality, or fitness for any particular purpose. The information in this document is subject to change without notice. Accton reserves the right to make revisions to this publication without obligation to notify any person or entity of any such changes.

Accton

International Headquarters
No. 1 Creation Road III,
Science-based Industrial Park
Hsinchu 300, Taiwan
Phone: 886-3-5770-270
Fax: 886-3-5770-267
Internet: support@accton.com.tw

Europe Headquarters
Edificio Conata II,
Calle Fructuós Gelabert 6-8, 2º, 4ª,
08970 - Sant Joan Despí,
Barcelona, Spain.
Phone: +34-93-477-4920
Fax: +34-93-477-3774

Asia Pacific Headquarters
1 Claymore Drive
#08-05/06 Orchard Towers (Rear Block)
Singapore 229594
Phone: +65 238 6556
Fax: +65 238 6466
Internet: www.acctontech.com

VS4512
VS4512DC
E112003-R01
150000041800A v1.0.4.0

Contents

Chapter 1: Introduction

This switch provides a broad range of features for Layer 2 switching. It includes a management agent that allows you to configure the features listed in this manual. The default configuration can be used for most of the features provided by this switch. However, there are many options that you should configure to maximize the switch's performance for your particular network environment.

Key Features

Feature	Description
Configuration Backup and Restore	Backup to TFTP server
Authentication	Console, Telnet, web – User name / password, RADIUS, TACACS+ Web – HTTPS; Telnet – SSH SNMP – Community strings, IP address filtering Port – IEEE 802.1x, MAC address filtering
DHCP Client	Supported
Port Configuration	Speed, duplex mode and flow control
Rate Limiting	Input and output rate limiting per port
Port Mirroring	One or more ports mirrored to single analysis port
Port Trunking	Supports 1 Gigabit trunk using either static or dynamic trunking (LACP)
Broadcast Storm Control	Supported
Static Address	Up to 8K MAC addresses in the forwarding table
IEEE 802.1D Bridge	Supports dynamic data switching and addresses learning
Store-and-Forward Switching	Supported to ensure wire-speed switching while eliminating bad frames
Spanning Tree Protocol	Supports standard STP and Rapid Spanning Tree Protocol (RSTP)
Virtual LANs	Up to 255 using IEEE 802.1Q, port-based, or private VLANs
Traffic Prioritization	Default port priority, traffic class map, queue scheduling, IP Precedence, or Differentiated Services Code Point (DSCP)
Multicast Filtering	Supports IGMP snooping and query

Description of Software Features

The switch provides a wide range of advanced performance enhancing features. Flow control eliminates the loss of packets due to bottlenecks caused by port saturation. Broadcast storm suppression prevents broadcast traffic storms from engulfing the network. Port-based VLANs provide traffic security and efficient use of network bandwidth. CoS priority queueing ensures the minimum delay for moving real-time multimedia data across the network. While multicast filtering provides support for real-time network applications. Some of the management features are briefly described below.

Configuration Backup and Restore – You can save the current configuration settings to a file on a TFTP server, and later download this file to restore the switch configuration settings.

Authentication – This switch authenticates management access via the console port, Telnet or web browser. User names and passwords can be configured locally or can be verified via a remote authentication server (i.e., RADIUS or TACACS+). Port-based authentication is also supported via the IEEE 802.1x protocol. This protocol uses the Extensible Authentication Protocol over LANs (EAPOL) to request user credentials from the 802.1x client, and then verifies the client’s right to access the network via an authentication server.

Other authentication options include HTTPS for secure management access via the web, SSH for secure management access over a Telnet-equivalent connection, IP address filtering for SNMP/web/Telnet management access, and MAC address filtering for port access.

Port Configuration – You can manually configure the speed, duplex mode, and flow control used on specific ports, or use auto-negotiation to detect the connection settings used by the attached device. Use the full-duplex mode on ports whenever possible to double the throughput of switch connections. Flow control should also be enabled to control network traffic during periods of congestion and prevent the loss of packets when port buffer thresholds are exceeded. The switch supports flow control based on the IEEE 802.3x standard.

Rate Limiting – This feature controls the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

Port Mirroring – The switch can unobtrusively mirror traffic from any port to a monitor port. You can then attach a protocol analyzer or RMON probe to this port to perform traffic analysis and verify connection integrity.

Port Trunking – Ports can be combined into an aggregate connection. Trunks can be manually set up or dynamically configured using IEEE 802.3ad Link Aggregation Control Protocol (LACP). The additional ports dramatically increase the throughput across any connection, and provide redundancy by taking over the load if a port in the trunk should fail. The switch supports one trunk with two Gigabit optional module ports.

Broadcast Storm Control – Broadcast suppression prevents broadcast traffic from overwhelming the network. When enabled on a port, the level of broadcast traffic passing through the port is restricted. If broadcast traffic rises above a pre-defined threshold, it will be throttled until the level falls back beneath the threshold.

Static Addresses – A static address can be assigned to a specific interface on this switch. Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table. Static addresses can be used to provide network security by restricting access for a known host to a specific port.

IEEE 802.1D Bridge – The switch supports IEEE 802.1D transparent bridging. The address table facilitates data switching by learning addresses, and then filtering or forwarding traffic based on this information. The address table supports up to 8K addresses.

Store-and-Forward Switching – The switch copies each frame into its memory before forwarding them to another port. This ensures that all frames are a standard Ethernet size and have been verified for accuracy with the cyclic redundancy check (CRC). This prevents bad frames from entering the network and wasting bandwidth.

To avoid dropping frames on congested ports, the switch provides 8 MB for frame buffering. This buffer can queue packets awaiting transmission on congested networks.

Spanning Tree Protocol – The switch supports these spanning tree protocols:

Spanning Tree Protocol (STP, IEEE 802.1D) – This protocol adds a level of fault tolerance by allowing two or more redundant connections to be created between a pair of LAN segments. When there are multiple physical paths between segments, this protocol will choose a single path and disable all others to ensure that only one route exists between any two stations on the network. This prevents the creation of network loops. However, if the chosen path should fail for any reason, an alternate path will be activated to maintain the connection.

Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w) – This protocol reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard. It is intended as a complete replacement for STP, but can still interoperate with switches running the older standard by automatically reconfiguring ports to STP-compliant mode if they detect STP protocol messages from attached devices.

Virtual LANs – The switch supports up to 255 VLANs. A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. The switch supports tagged VLANs based on the IEEE 802.1Q standard. Members of VLAN groups can be manually assigned to a specific set of VLANs. This allows the switch to restrict traffic to the VLAN groups to which a user has been assigned. By segmenting your network into VLANs, you can:

- Eliminate broadcast storms which severely degrade performance in a flat network.
- Simplify network management for node changes/moves by remotely configuring VLAN membership for any port, rather than having to manually change the network connection.
- Provide data security by restricting all traffic to the originating VLAN.
- Use private VLANs to restrict traffic to pass only between data ports and the uplink ports, thereby isolating adjacent ports within the same VLAN, and allowing you to limit the total number of VLANs that need to be configured.

Traffic Prioritization – This switch prioritizes each packet based on the required level of service, using four priority queues with strict or Weighted Round Robin Queuing. It uses IEEE 802.1p and 802.1Q tags to prioritize incoming traffic based on input from the end-station application. These functions can be used to provide independent priorities for delay-sensitive data and best-effort data.

This switch also supports several common methods of prioritizing layer 3/4 traffic to meet application requirements. Traffic can be prioritized based on the priority bits in the IP frame’s Type of Service (ToS) octet. When these services are enabled, the priorities are mapped to a Class of Service value by the switch, and the traffic then sent to the corresponding output queue.

Multicast Filtering – Specific multicast traffic can be assigned to its own VLAN to ensure that it does not interfere with normal network traffic and to guarantee real-time delivery by setting the required priority level for the designated VLAN. The switch uses IGMP Snooping and Query to manage multicast group registration.

System Defaults

The switch's system defaults are provided in the configuration file "Factory_Default_Config.cfg." To reset the switch defaults, this file should be set as the startup configuration file (page 3-17).

The following table lists some of the basic system defaults.

Function	Parameter	Default
IP Settings	Management VLAN	1
	DHCP	Enabled
	BOOTP	Disabled
	User Specified	Disabled
	IP Address	0.0.0.0
	Subnet Mask	255.0.0.0
	Default Gateway	0.0.0.0
Console Port Connection	Baud Rate	9600
	Data bits	8
	Stop bits	1
	Parity	none
	Local Console Timeout	0 (disabled)
Authentication	Privileged Exec Level	Username "admin" Password "admin"
	Normal Exec Level	Username "guest" Password "guest"
	Enable Privileged Exec from Normal Exec Level	Password "super"
	RADIUS Authentication	Disabled
	TACACS Authentication	Disabled
	802.1x Port Authentication	Disabled
	SSL	Enabled
	HTTPS	Enabled
	SSH version 2.0	Enabled
	Port Security	Disabled

Function	Parameter	Default
Web Management	HTTP Server	Enabled
	HTTP Port Number	80
	HTTP Secure Server	Enabled
	HTTP Secure Port Number	443
SNMP	Community Strings	“public” (read only) “private” (read/write)
	Traps	Authentication traps: enabled Link-up-down events: enabled
	IP Filtering	Disabled
Port Configuration	Admin Status	Enabled
	Auto-negotiation	Enabled
	Flow Control	Disabled
	Port Capability	100BASE-TX – 10 Mbps half duplex 10 Mbps full duplex 100 Mbps half duplex 100 Mbps full duplex Full-duplex flow control disabled Symmetric flow control disabled
	Module Port Capability	1000BASE-T/SX/LX/LH – 1000 Mbps full duplex Full-duplex flow control disabled Symmetric flow control disabled
Rate Limiting	Input and output limits	Disabled
Port Trunking	Static Trunks	None
	LACP (all ports)	Disabled
Broadcast Storm Protection	Status	Enabled (all ports)
	Broadcast Limit Rate	500 packets per second
Spanning Tree Protocol	Status	Enabled (Defaults: All values based on IEEE 802.1w)
	Fast Forwarding (Edge Port)	Disabled
Address Table	Aging Time	300 seconds
Virtual LANs	Default VLAN	1
	PVID	1

Function	Parameter	Default
	Acceptable Frame Type	All
	Ingress Filtering	Disabled
	Switchport Mode (Egress Mode)	Hybrid: tagged/untagged frames
Traffic Prioritization	Ingress Port Priority	0
	Weighted Round Robin	Queue: 0:1 1:4 2:16 3:64
	IP Precedence Priority	Disabled
	IP DSCP Priority	Disabled
IP Settings	IP Address	0.0.0.0
	Subnet Mask	255.0.0.0
	Default Gateway	0.0.0.0
	DHCP	Client: Disabled
	BOOTP	Disabled
DNS Server	Lookup	Disabled
Multicast Filtering	IGMP Snooping	Snooping: Enabled Querier: Enabled
System Log	Status	Enabled
	Messages Logged	Levels 0-7 (all)
	Messages Logged to Flash	Levels 0-3
SMTP Email Alerts	Event Handler	Disabled
SNTP	Clock Synchronization	Disabled

Chapter 2: Initial Configuration

Connecting to the Switch

Configuration Options

The switch includes a built-in network management agent. The agent offers a variety of management options, including SNMP, RMON and a Web-based interface. A PC may also be connected directly to the switch for configuration and monitoring via a command line interface (CLI).

Note: The IP address for this switch is assigned by DHCP by default. To change this address, see “Setting an IP Address” on page 2-4.

The switch’s HTTP Web agent allows you to configure switch parameters, monitor port connections, and display statistics using a standard Web browser such as Netscape Navigator version 6.2 and higher or Microsoft IE version 5.0 and higher. The switch’s Web management interface can be accessed from any computer attached to the network.

The CLI program can be accessed by a direct connection to the RS-232 serial console port on the switch, or remotely by a Telnet connection over the network.

The switch’s management agent also supports SNMP (Simple Network Management Protocol). This SNMP agent permits the switch to be managed from any system in the network using network management software such as AccView or HP OpenView.

The switch’s Web interface, CLI configuration program, and SNMP agent allow you to perform the following management functions:

- Set user names and passwords for up to 16 users
- Set an IP interface for a management VLAN
- Configure SNMP parameters
- Enable/disable any port
- Set the speed/duplex mode for any port
- Configure the bandwidth of any port by limiting input or output rates
- Configure up to 255 IEEE 802.1Q VLANs
- Configure IGMP multicast filtering
- Upload and download system firmware via TFTP
- Upload and download switch configuration files via TFTP
- Configure Spanning Tree parameters
- Configure Class of Service (CoS) priority queuing
- Configure one trunk with two Gigabit optional module ports
- Enable port mirroring

- Globally set broadcast storm control
- Display system information and statistics

Required Connections

The switch provides an RS-232 serial port that enables a connection to a PC or terminal for monitoring and configuring the switch. A null-modem console cable is provided with the switch.

Attach a VT100-compatible terminal, or a PC running a terminal emulation program to the switch. You can use the console cable provided with this package, or use a null-modem cable that complies with the wiring assignments shown in the Installation Guide.

To connect a terminal to the console port, complete the following steps:

1. Connect the console cable to the serial port on a terminal, or a PC running terminal emulation software, and tighten the captive retaining screws on the DB-9 connector.
2. Connect the other end of the cable to the RS-232 serial port on the switch.
3. Make sure the terminal emulation software is set as follows:
   - Select the appropriate serial port (COM port 1 or COM port 2).
   - Set to any of the following baud rates: 9600, 19200, 38400, 57600, 115200 (Note: Set to 9600 baud if want to view all the system initialization messages.)
   - Set the data format to 8 data bits, 1 stop bit, and no parity.
   - Set flow control to none.
   - Set the emulation mode to VT100.
   - When using HyperTerminal, select Terminal keys, not Windows keys.

Notes: **1.** When using HyperTerminal with Microsoft® Windows® 2000, make sure that you have Windows 2000 Service Pack 2 or later installed. Windows 2000 Service Pack 2 fixes the problem of arrow keys not functioning in HyperTerminal's VT100 emulation. See www.microsoft.com for information on Windows 2000 service packs.

2. Refer to “Line Commands” on page 4-9 for a complete description of console configuration options.

3. Once you have set up the terminal correctly, the console login screen will be displayed.

For a description of how to use the CLI, see “Using the Command Line Interface” on page 4-1. For a list of all the CLI commands and detailed information on using the CLI, refer to “Command Groups” on page 4-8.

Remote Connections

Prior to accessing the switch's onboard agent via a network connection, you must first configure it with a valid IP address, subnet mask, and default gateway using a console connection, DHCP or BOOTP protocol.

The IP address for this switch is assigned by DHCP by default. To manually configure this address or enable dynamic address assignment via DHCP or BOOTP, see "Setting an IP Address" on page 2-4.

Note: This switch supports four concurrent Telnet sessions.

After configuring the switch's IP parameters, you can access the onboard configuration program from anywhere within the attached network. The onboard configuration program can be accessed using Telnet from any computer attached to the network. The switch can also be managed by any computer using a web browser (Internet Explorer 5.0 or above, or Netscape Navigator 6.2 or above), or from a network computer using SNMP network management software.

Note: The onboard program only provides access to basic configuration functions. To access the full range of SNMP management functions, you must use SNMP-based network management software.

Basic Configuration

Console Connection

The CLI program provides two different command levels — normal access level (Normal Exec) and privileged access level (Privileged Exec). The commands available at the Normal Exec level are a limited subset of those available at the Privileged Exec level and allow you to only display information and use basic utilities. To fully configure the switch parameters, you must access the CLI at the Privileged Exec level.

Access to both CLI levels are controlled by user names and passwords. The switch has a default user name and password for each level. To log into the CLI at the Privileged Exec level using the default user name and password, perform these steps:

1. To initiate your console connection, press <Enter>. The "User Access Verification" procedure starts.
2. At the Username prompt, enter "admin."
3. At the Password prompt, also enter "admin." (The password characters are not displayed on the console screen.)
4. The session is opened and the CLI displays the "Console#" prompt indicating you have access at the Privileged Exec level.

Setting Passwords

Note: If this is your first time to log into the CLI program, you should define new passwords for both default user names using the “username” command, record them and put them in a safe place.

Passwords can consist of up to 8 alphanumeric characters and are case sensitive. To prevent unauthorized access to the switch, set the passwords as follows:

1. Open the console interface with the default user name and password “admin” to access the Privileged Exec level.
2. Type “configure” and press <Enter>.
3. Type “username guest password 0 *password*,” for the Normal Exec level, where *password* is your new password. Press <Enter>.
4. Type “username admin password 0 *password*,” for the Privileged Exec level, where *password* is your new password. Press <Enter>.

```
Username: admin
Password:

       CLI session with the VDSL 4Band Switch is opened.
      To end the CLI session, enter [Exit].

Console#configure
Console(config)#username guest password 0 [password]
Console(config)#username admin password 0 [password]
Console(config)#
```

Setting an IP Address

You must establish IP address information for the switch to obtain management access through the network. This can be done in either of the following ways:

Manual — You have to input the information, including IP address and subnet mask. If your management station is not in the same IP subnet as the switch, you will also need to specify the default gateway router.

Dynamic — The switch sends IP configuration requests to BOOTP or DHCP address allocation servers on the network.

Manual Configuration

You can manually assign an IP address to the switch. You may also need to specify a default gateway that resides between this device and management stations that exist on another network segment. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the CLI program.

Note: The IP address for this switch is assigned by DHCP by default.

Before you can assign an IP address to the switch, you must obtain the following information from your network administrator:

- IP address for the switch
- Default gateway for the network
- Network mask for this network

To assign an IP address to the switch, complete the following steps:

1. From the Privileged Exec level global configuration mode prompt, type “interface vlan 1” to access the interface-configuration mode. Press <Enter>.
2. Type “ip address *ip-address netmask*,” where “ip-address” is the switch IP address and “netmask” is the network mask for the network. Press <Enter>.
3. Type “exit” to return to the global configuration mode prompt. Press <Enter>.
4. To set the IP address of the default gateway for the network to which the switch belongs, type “ip default-gateway *gateway*,” where “gateway” is the IP address of the default gateway. Press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 192.168.1.254
Console(config)#
```

Dynamic Configuration

If you select the “bootp” or “dhcp” option, IP will be enabled but will not function until a BOOTP or DHCP reply has been received. You therefore need to use the “ip dhcp restart client” command to start broadcasting service requests. Requests will be sent periodically in an effort to obtain IP configuration information. (BOOTP and DHCP values can include the IP address, subnet mask, and default gateway.)

If the “bootp” or “dhcp” option is saved to the startup-config file (step 6), then the switch will start broadcasting service requests as soon as it is powered on.

To automatically configure the switch by communicating with BOOTP or DHCP address allocation servers on the network, complete the following steps:

1. From the Global Configuration mode prompt, type “interface vlan 1” to access the interface-configuration mode. Press <Enter>.
2. At the interface-configuration mode prompt, use one of the following commands:
    - To obtain IP settings via DHCP, type “ip address dhcp” and press <Enter>.
    - To obtain IP settings via BOOTP, type “ip address bootp” and press <Enter>.
3. Type “end” to return to the Privileged Exec mode. Press <Enter>.
4. Type “ip dhcp restart client” to begin broadcasting service requests.
   Press <Enter>.

5. Wait a few minutes, and then check the IP configuration settings by typing the “show ip interface” command. Press <Enter>.

6. Then save your configuration changes by typing “copy running-config startup-config.” Enter the startup file name and press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#end
Console#ip dhcp restart client
Console#show ip interface
 IP address and netmask: 192.168.1.54 255.255.255.0 on VLAN 1,
 and address mode: User specified.
Console#copy running-config startup-config
Startup configuration file name []: startup
\Write to FLASH Programming.

\Write to FLASH finish.
Success.
```

Enabling SNMP Management Access

The switch can be configured to accept management commands from Simple Network Management Protocol (SNMP) applications such as AccView. You can configure the switch to (1) respond to SNMP requests or (2) generate SNMP traps.

When SNMP management stations send requests to the switch (either to return information or to set a parameter), the switch provides the requested data or sets the specified parameter. The switch can also be configured to send information to SNMP managers (without being requested by the managers) through trap messages, which inform the manager that certain events have occurred.

Community Strings

Community strings are used to control management access to SNMP stations, as well as to authorize SNMP stations to receive trap messages from the switch. You therefore need to assign community strings to specified users or user groups, and set the access level.

The default strings are:

- **public** - with read-only access. Authorized management stations are only able to retrieve MIB objects.
- **private** - with read-write access. Authorized management stations are able to both retrieve and modify MIB objects.

Note: If you do not intend to utilize SNMP, we recommend that you delete both of the default community strings. If there are no community strings, then SNMP management access to the switch is disabled.

To prevent unauthorized access to the switch via SNMP, it is recommended that you change the default community strings.

To configure a community string, complete the following steps:

1. From the Privileged Exec level global configuration mode prompt, type “snmp-server community *string mode*,” where “string” is the community access string and “mode” is **rw** (read/write) or **ro** (read only). Press <Enter>. (Note that the default mode is read only.)
2. To remove an existing string, simply type “no snmp-server community *string*,” where “string” is the community access string to remove. Press <Enter>.

```
Console(config)#snmp-server community admin rw
Console(config)#snmp-server community private
Console(config)#
```

Trap Receivers

You can also specify SNMP stations that are to receive traps from the switch.

To configure a trap receiver, complete the following steps:

1. From the Privileged Exec level global configuration mode prompt, type “snmp-server host *host-address community-string*,” where “host-address” is the IP address for the trap receiver and “community-string” is the string associated with that host. Press <Enter>.
2. In order to configure the switch to send SNMP notifications, you must enter at least one snmp-server enable traps command. Type “snmp-server enable traps *type*,” where “type” is either **authentication** or **link-up-down**. Press <Enter>.

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

Saving Configuration Settings

Configuration commands only modify the running configuration file and are not saved when the switch is rebooted. To save all your configuration changes in nonvolatile storage, you must copy the running configuration file to the start-up configuration file using the “copy” command.

To save the current configuration settings, enter the following command:

1. From the Privileged Exec mode prompt, type “copy running-config startup-config” and press <Enter>.
2. Enter the name of the start-up file. Press <Enter>.

```
Console#copy running-config startup-config
Startup configuration file name []: startup
\Write to FLASH Programming.

\Write to FLASH finish.
Success.

Console#
```

Managing System Files

The switch’s flash memory supports three types of system files that can be managed by the CLI program, Web interface, or SNMP. The switch’s file system allows files to be uploaded and downloaded, copied, deleted, and set as a start-up file.

The three types of files are:

- **Configuration** — This file stores system configuration information and is created when configuration settings are saved. Saved configuration files can be selected as a system start-up file or can be uploaded via TFTP to a server for backup. A file named “Factory_Default_Config.cfg” contains all the system default settings and cannot be deleted from the system. See “Saving or Restoring Configuration Settings” on page 3-16 for more information.

- **Operation Code** — System software that is executed after boot-up, also known as run-time code. This code runs the switch operations and provides the CLI and Web management interfaces. See “Managing Firmware” on page 3-14 for more information.

- **Diagnostic Code** — Software that is run during system boot-up, also known as POST (Power On Self-Test).

Due to the size limit of the flash memory, the switch supports only two operation code files. However, you can have as many diagnostic code files and configuration files as available flash memory space allows.

In the system flash memory, one file of each type must be set as the start-up file. During a system boot, the diagnostic and operation code files set as the start-up file are run, and then the start-up configuration file is loaded.

Note that configuration files should be downloaded using a file name that reflects the contents or usage of the file settings. If you download directly to the running-config, the system will reboot, and the settings will have to be copied from the running-config to a permanent file.

Chapter 3: Configuring the Switch

Using the Web Interface

This switch provides an embedded HTTP Web agent. Using a Web browser you can configure the switch and view statistics to monitor network activity. The Web agent can be accessed by any computer on the network using a standard Web browser (Internet Explorer 5.0 or above, or Netscape Navigator 6.2 or above).

Note: You can also use the Command Line Interface (CLI) to manage the switch over a serial connection to the console port or via Telnet. For more information on using the CLI, refer to Chapter 4: "Command Line Interface."

Prior to accessing the switch from a Web browser, be sure you have first performed the following tasks:

1. Configure the switch with a valid IP address, subnet mask, and default gateway using an out-of-band serial connection, BOOTP or DHCP protocol. (See "Setting an IP Address" on page 2-4.)

2. Set user names and passwords using an out-of-band serial connection. Access to the Web agent is controlled by the same user names and passwords as the onboard configuration program. (See "Setting Passwords" on page 2-4.)

3. After you enter a user name and password, you will have access to the system configuration program.

Notes:

1. You are allowed three attempts to enter the correct password; on the third failed attempt the current connection is terminated.

2. If you log into the Web interface as guest (Normal Exec level), you can view the configuration settings or change the guest password. If you log in as "admin" (Privileged Exec level), you can change the settings on any page.

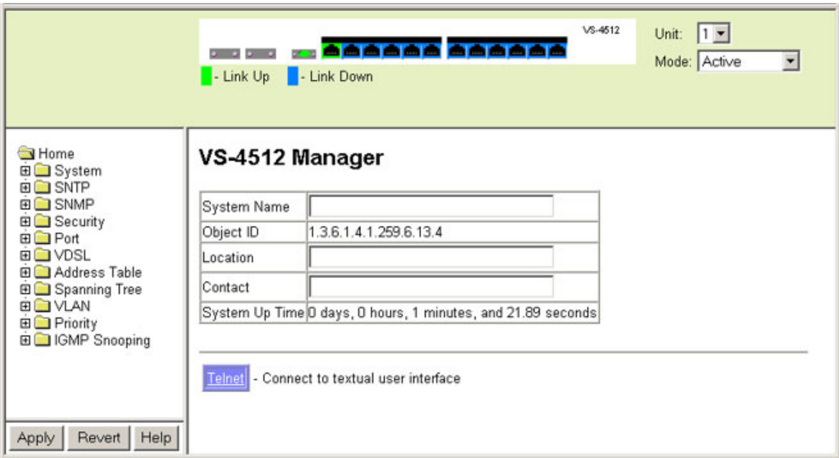
3. If the path between your management station and this switch does not pass through any device that uses the Spanning Tree Algorithm, then you can set the switch port attached to your management station to fast forwarding (i.e., enable Admin Edge Port) to improve the switch's response time to management commands issued through the web interface. See "Configuring Interface Settings" on page 3-81.

Navigating the Web Browser Interface

To access the web-browser interface you must first enter a user name and password. The administrator has Read/Write access to all configuration parameters and statistics. The default user name and password for the administrator is “admin.”

Home Page

When your web browser connects with the switch’s web agent, the home page is displayed as shown below. The home page displays the Main Menu on the left side of the screen and System Information on the right side. The Main Menu links are used to navigate to other menus, and display configuration parameters and statistics.



Unit: 1

Mode: Active

VS-4512 Manager

System Name	
Object ID	1.3.6.1.4.1.259.6.13.4
Location	
Contact	
System Up Time	0 days, 0 hours, 1 minutes, and 21.89 seconds

Telnet - Connect to textual user interface

Configuration Options

Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, be sure to click on the Apply or Apply Changes button to confirm the new setting. The following table summarizes the web page configuration buttons.

Button	Action
Revert	Cancels specified values and restores current values prior to pressing Apply or Apply Changes.
Refresh	Immediately updates values for the current page.
Apply	Sets specified values to the system.
Apply Changes	Sets specified values to the system.

Notes: **1.** To ensure proper screen refresh, be sure that Internet Explorer 5.x is configured as follows: Under the menu “Tools / Internet Options / General / Temporary Internet Files / Settings,” the setting for item “Check for newer versions of stored pages” should be “Every visit to the page.”

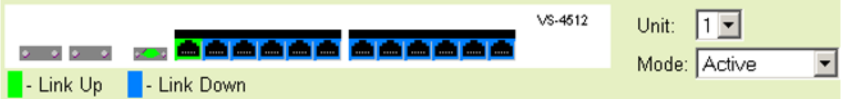
2. When using Internet Explorer 5.0, you may have to manually refresh the screen after making configuration changes by pressing the browser’s refresh button.

Panel Display

The web agent displays an image of the switch’s ports. The items in the Mode drop-down menu are:

Item	Description	Values
Active	Displays the link status of the ports	Green — Link Up, Blue — Link Down
Duplex	Displays the duplex mode of the ports	Green — Disabled, Blue — Enabled
Switch Information	Shows port flow control status	Green — Half Duplex , Blue — Full Duplex

Clicking on the image of a port opens the Port Configuration page as described on page 3-42.



🟩 - Link Up 🟦 - Link Down

Unit: 1

Mode: Active

Main Menu

Using the onboard web agent, you can define system parameters, manage and control the switch and all its ports, or monitor network conditions. The following table briefly describes the selections available from this program.

Menu	Description	Page
System		3-7
System Information	Provides basic system description, including contact information	3-7
Switch Information	Shows the number of ports, hardware/firmware version numbers, and power status	3-9
Bridge Extension	Shows the bridge extension parameters	3-10
IP Configuration	Sets the IP address for management access	3-11
Fan Status	Displays the status of the switch fans	3-14
Firmware	Manages code image files	3-14
Configuration	Manages switch configuration files	3-16
Reset	Restarts the switch	3-18

Menu	Description	Page
SNTP		3-18
Configuration	Configures SNTP client settings, including broadcast mode or a specified list of servers	3-18
Clock Time Zone	Sets the local time zone for the system clock	3-19
SNMP		3-20
Configuration	Configures community strings and related trap functions	3-21
IP Filtering	Sets IP addresses of clients allowed management access	3-23
Security		3-24
Passwords	Assigns a new password for the current user	3-24
Authentication Settings	Configures authentication sequence, RADIUS and TACACS	3-25
Telnet Settings	Enables to the access the onboard configuration program by a VT100 compatible device attached to the server's serial port.	3-28
HTTPS Settings	Configures secure HTTP settings	3-28
SSH		3-30
Settings	Configures Secure Shell server settings	3-30
Host-Key Settings	Generates the host key pair (public and private)	3-30
Port Security	Configures per port security, including status, response for security breach, and maximum allowed MAC addresses	3-31
802.1x	Port authentication	3-33
Information	Displays global configuration settings	3-34
Configuration	Configures protocol parameters	3-36
Port Configuration	Sets the authentication mode for individual ports	3-37
Statistics	Displays protocol statistics for the selected port	3-38
Port		3-40
Port Information	Displays port connection status	3-40
Trunk Information	Displays trunk connection status	3-40
Port Configuration	Configures port connection settings	3-42
Trunk Configuration	Configures trunk connection settings	3-42
Trunk Membership	Specifies ports to group into static trunks	3-45
LACP Configuration	Allows ports to dynamically join trunks	3-46
Broadcast Control	Globally sets the broadcast storm threshold for the switch	3-48
Mirror Port Configuration	Sets the source and target ports for mirroring	3-49

Menu	Description	Page
Rate Limit		3-50
Input Port Configuration	Sets the input rate limit for each port	3-50
Input Trunk Configuration	Sets the input rate limit for each trunk	3-50
Output Port Configuration	Sets the output rate limit for each port	3-50
Output Trunk Configuration	Sets the output rate limit for each trunk	3-50
Port Statistics	Lists Ethernet and RMON port statistics	3-51
VDSL		3-56
Global Configuration	Batch assigns profiles for speed and distance range to all the VDSL ports on the switch	3-56
Port Configuration	Configures port connection settings	3-58
Port Link Status	Displays information on the link status of individual VDSL ports	3-60
Port Ethernet Statistics	Displays Ethernet statistics for individual switch VDSL ports and linked CPE Ethernet ports	3-62
Line Configuration	Configures line connection settings	3-64
Interface Information	Displays physical interface and channel interface information	3-65
Performance Monitor Information	Displays line and channel performance data information since the switch was last reset, during the current 15 minute interval, and during the current day.	3-66
Performance Monitor History	Displays line and channel performance data information during selected 15 minute intervals over the last 24 hours of switch operation, and during selected 1-day intervals from the current day to 30 days ago.	3-68
Address Table		3-70
Static Addresses	Displays entries for interface, address or VLAN	3-70
Dynamic Addresses	Displays or edits static entries in the Address Table	3-71
Address Aging	Sets timeout for dynamically learned entries	3-72
Spanning Tree		3-73
STA		3-73
Information	Displays STA values used for the bridge	3-74
Configuration	Configures global bridge settings for STA and RSTP	3-76
Port Information	Displays individual port settings for STA	3-78
Trunk Information	Displays individual trunk settings for STA	3-78
Port Configuration	Configures individual port settings for STA	3-81
Trunk Configuration	Configures individual trunk settings for STA	3-81

Menu	Description	Page
VLAN		3-83
802.1Q VLAN		
Basic Information	Displays information on the VLAN type supported by this switch	3-85
Current Table	Shows the current port members of each VLAN and whether or not the port is tagged or untagged	3-86
Static List	Used to create or remove VLAN groups	3-88
Static Table	Modifies the settings for an existing VLAN	3-89
Static Membership	Configures membership type for interfaces, including tagged, untagged or forbidden	3-90
Port Configuration	Specifies default PVID and VLAN attributes	3-91
Trunk Configuration	Specifies default trunk VID and VLAN attributes	3-91
Private VLAN		3-94
Private VLAN Status	Enables or disables the Private VLAN feature	3-94
Private VLAN Link Status	Configures ports as downlink or uplink ports. Traffic from downlink ports can only be forwarded to, and from, the uplink ports	3-95
Priority		3-96
Default Port Priority	Sets the default priority for each port	3-96
Default Trunk Priority	Sets the default priority for each trunk	3-96
Traffic Classes	Maps IEEE 802.1p priority tags to output queues	3-97
Traffic Classes Status	Enables/disables traffic class priorities (not implemented)	NA
Queue Mode	Sets queue mode to strict priority or Weighted Round-Robin	3-99
Queue Scheduling	Configures Weighted Round Robin queueing	3-100
IP Precedence/ DSCP Priority Status	Globally selects IP Precedence or DSCP Priority, or disables both.	3-101
IP Precedence Priority	Sets IP Type of Service priority, mapping the precedence tag to a class-of-service value	3-101
IP DSCP Priority	Sets IP Differentiated Services Code Point priority, mapping a DSCP tag to a class-of-service value	3-103
IP Port Priority Status	Enables/disables Port Priority status	3-104
IP Port Priority	Maps IP ports (TCP/UDP ports) to the switch’s 4 traffic class queues	3-104
Copy Settings	Allows you to copy the priority settings from a selected port or trunk to another selected port or trunk	3-106

Menu	Description	Page
IGMP Snooping		3-106
IGMP Configuration	Enables multicast filtering; configures parameters for multicast query	3-107
Multicast Router Port Information	Displays the ports that are attached to a neighboring multicast router for each VLAN ID	3-109
Static Multicast Router Port Configuration	Assigns ports that are attached to a neighboring multicast router	3-110
IP Multicast Registration Table	Displays all multicast groups active on this switch, including multicast IP addresses and VLAN ID	3-111
IGMP Member Port Table	Indicates multicast addresses associated with the selected VLAN	3-112

Basic Configuration

Displaying System Information

You can easily identify the system by displaying the device name, location and contact information.

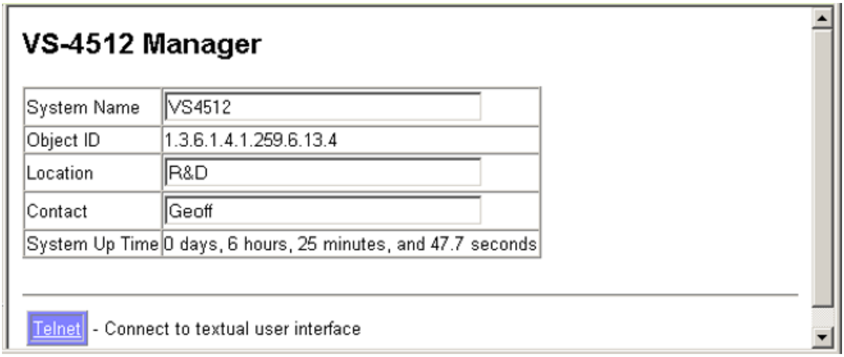
Field Attributes

- **System Name** – Name assigned to the switch system.
- **Object ID** – MIB II object ID for switch’s network management subsystem.
- **Location** – Specifies the system location.
- **Contact** – Administrator responsible for the system.
- **System Up Time** – Length of time the management agent has been up.

These additional parameters are displayed for the CLI.

- **MAC Address** – The physical layer address for this switch.
- **Web server** – Shows if management access via HTTP is enabled.
- **Web server port** – Shows the TCP port number used by the web interface.
- **Web secure server** – Shows if management access via HTTPS is enabled.
- **Web secure server port** – Shows the TCP port used by the HTTPS interface.
- **POST result** – Shows results of the power-on self-test

Web – Click System, System Information. Specify the system name, location, and contact information for the system administrator, then click Apply. (This page also includes a Telnet button that allows access to the Command Line Interface via Telnet.)



VS-4512 Manager

System Name	VS4512
Object ID	1.3.6.1.4.1.259.6.13.4
Location	R&D
Contact	Geoff
System Up Time	0 days, 6 hours, 25 minutes, and 47.7 seconds

CLI – Specify the hostname, location and contact information.

```
Console(config)#hostname VS-4512                                          4-24
Console(config)#snmp-server location R&D                                  4-79
Console(config)#snmp-server contact Geoff                                 4-79
Console(config)#exit
Console#show system                                                       4-55
System description: VS-4512
System OID string: 1.3.6.1.4.1.259.6.13.4
System information
 System Up time: 0 days, 6 hours, 7 minutes, and 9.51 seconds
 System Name            : VS-4512
 System Location        : R&D
 System Contact         : Geoff
 MAC address            : 00-01-00-02-00-03
 Web server             : enable
 Web server port        : 80
 Web secure server      : enable
 Web secure server port : 443
 Telnet server          : enable
 POST result
DUMMY Test 1.................PASS
UART LOOP BACK Test..........PASS
DRAM Test....................PASS
Timer Test...................PASS
RTC Test.....................PASS
PCI Device   Test............PASS
Firmware DownloadPASS
Switch Int Loopback test.....PASS

Done All Pass.logy change notification.
Console#
```

Displaying Switch Hardware/Software Versions

Use the Switch Information page to display hardware/firmware version numbers for the main board and management software, as well as the power status of the system.

Field Attributes

Main Board

- **Serial Number** – The serial number of the switch.
- **Number of Ports** – Number of built-in RJ-45 ports and expansion ports.
- **Hardware Version** – Hardware version of the main board.
- **Internal Power Status** – Displays the status of the internal power supply.
- **Redundant Power Status*** – Displays the status of the redundant power supply. This will display as “not present” since this switch has no redundant power supply.

* CLI only.

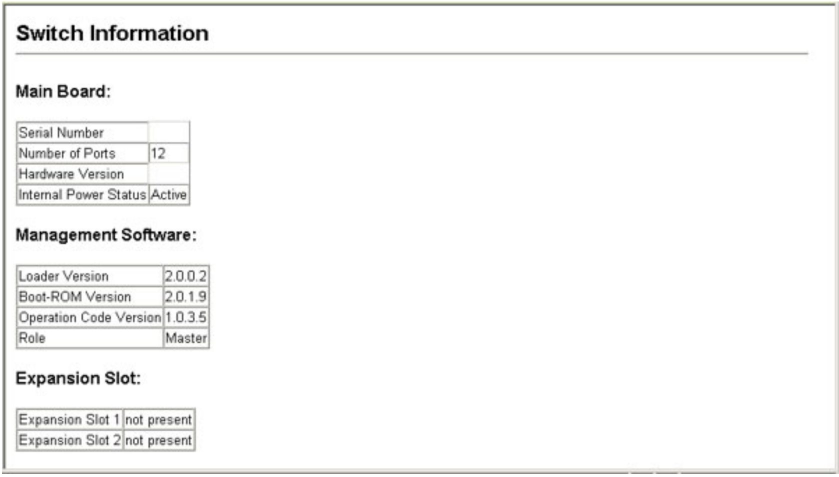
Management Software

- **Loader Version** – Version number of loader code.
- **Boot-ROM Version** – Version of Power-On Self-Test (POST) and boot code.
- **Operation Code Version** – Version number of runtime code.
- **Role** – Shows that this switch is operating as Master (i.e., operating stand-alone).

Expansion Slot

- **Expansion Slot 1/2** – Slots for extender modules.

Web – Click System, Switch Information.



Switch Information

Main Board:

Serial Number	
Number of Ports	12
Hardware Version	
Internal Power Status	Active

Management Software:

Loader Version	2.0.0.2
Boot-ROM Version	2.0.1.9
Operation Code Version	1.0.3.5
Role	Master

Expansion Slot:

Expansion Slot 1	not present
Expansion Slot 2	not present

CLI – Use the following command to display version information.

```
Console#show version                                                        4-56
Unit1
 Serial number           :
 Service tag             :
 Hardware version        :
 Module A type           :not present
 Module B type           :not present
 Number of ports         :12
 Main power status       :
 Redundant power status :
Agent(master)
 Unit id                 :1
 Loader version          :2.0.0.2
 Boot rom version        :2.0.1.9
 Operation code version :1.0.3.5
Console#
```

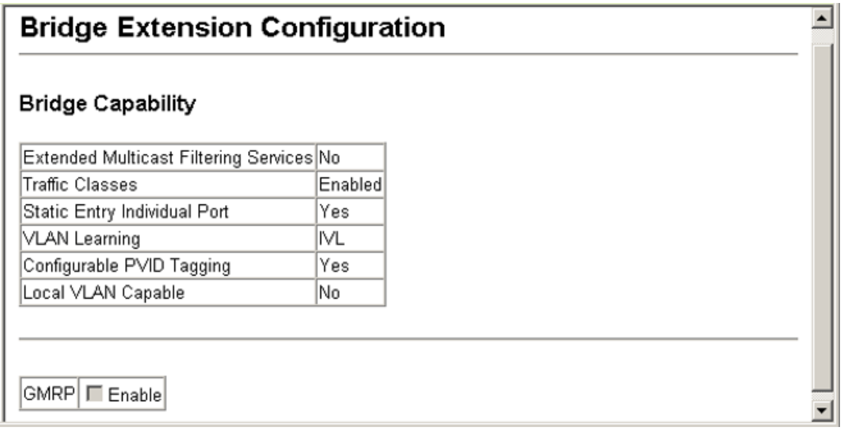
Displaying Bridge Extension Capabilities

The Bridge MIB includes extensions for managed devices that support Multicast Filtering, Traffic Classes, and Virtual LANs. You can access these extensions to display default settings for the key variables.

Field Attributes

- **Extended Multicast Filtering Services** – This switch does not support the filtering of individual multicast addresses based on GMRP (GARP Multicast Registration Protocol).
- **Traffic Classes** – This switch provides mapping of user priorities to multiple traffic classes. (Refer to “Class of Service Configuration” on page 3-96.) Note that Traffic classes is always enabled in this switch, it cannot be disabled.
- **Static Entry Individual Port** – This switch allows static filtering for unicast and multicast addresses. (Refer to “Setting Static Addresses” on page 3-70.)
- **VLAN Learning** – This switch uses Independent VLAN Learning (IVL), where each port maintains its own filtering database.
- **Configurable PVID Tagging** – This switch allows you to override the default Port VLAN ID (PVID used in frame tags) and egress status (VLAN-Tagged or Untagged) on each port. (Refer to “VLAN Configuration” on page 3-83.)
- **GMRP** – GARP Multicast Registration Protocol (GMRP) allows network devices to register endstations with multicast groups. This switch does not support GMRP; it uses the Internet Group Management Protocol (IGMP) to provide automatic multicast filtering.

Web – Click System, Bridge Extension.



Bridge Extension Configuration

Bridge Capability

Extended Multicast Filtering Services	No
Traffic Classes	Enabled
Static Entry Individual Port	Yes
VLAN Learning	IVL
Configurable PVID Tagging	Yes
Local VLAN Capable	No

GMRP □ Enable

CLI – Enter the following command.

```
Console#show bridge-ext                                                  4-144
 Max support vlan numbers: 255
 Max support vlan ID: 4093
 Extended multicast filtering services: No
 Static entry individual port: Yes
 VLAN learning: IVL
 Configurable PVID tagging: Yes
 Local VLAN capable: Yes
 Traffic classes: Enabled
 GMRP: Disabled
Console#
```

Setting the Switch’s IP Address

An IP address may be used for management access to the switch over your network. By default, the switch uses DHCP to assign IP settings to VLAN 1 on the switch. If you wish to manually configure IP settings, you need to change the switch’s user-specified defaults (IP address 0.0.0.0 and netmask 255.0.0.0) to values that are compatible with your network. You may also need to establish a default gateway between the switch and management stations that exist on another network segment.

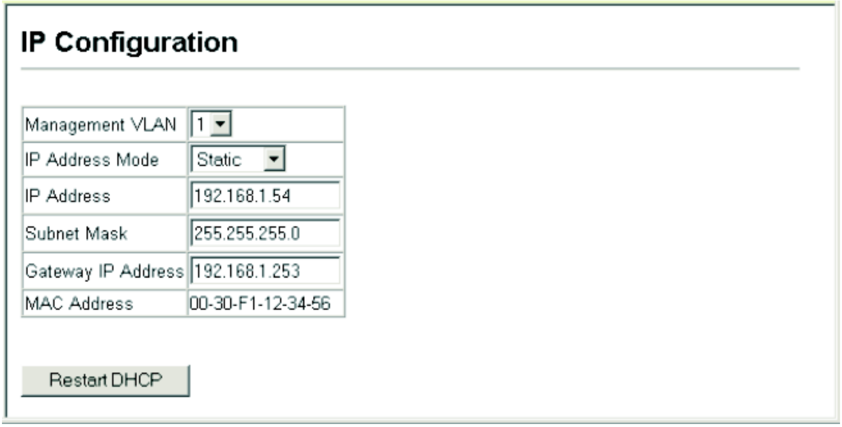
You can manually configure a specific IP address, or direct the device to obtain an address from a BOOTP or DHCP server when it is powered on. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the CLI program.

Command Attributes

- **Management VLAN** – ID of the configured VLAN (1-4093, no leading zeroes). By default, all ports on the switch are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address.
- **IP Address Mode** – Specifies whether IP functionality is enabled via manual configuration (Static), Dynamic Host Configuration Protocol (DHCP), or Boot Protocol (BOOTP). If DHCP/BOOTP is enabled, IP will not function until a reply has been received from the server. Requests will be broadcast periodically by the switch for an IP address. (DHCP/BOOTP values can include the IP address, subnet mask, and default gateway.)
- **IP Address** – Address of the VLAN interface that is allowed management access. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. (Default: 0.0.0.0)
- **Subnet Mask** – This mask identifies the host address bits used for routing to specific subnets. (Default: 255.0.0.0)
- **Gateway IP Address** – IP address of the gateway router between this device and management stations that exist on other network segments. (Default: 0.0.0.0)
- **MAC Address** – The physical layer address for this switch.

Manual Configuration

Web – Click System, IP Configuration. Select the VLAN through which the management station is attached, set the IP Address Mode to “Static,” enter the IP address, subnet mask and gateway, then click Apply.



IP Configuration

Management VLAN	1
IP Address Mode	Static
IP Address	192.168.1.54
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.253
MAC Address	00-30-F1-12-34-56

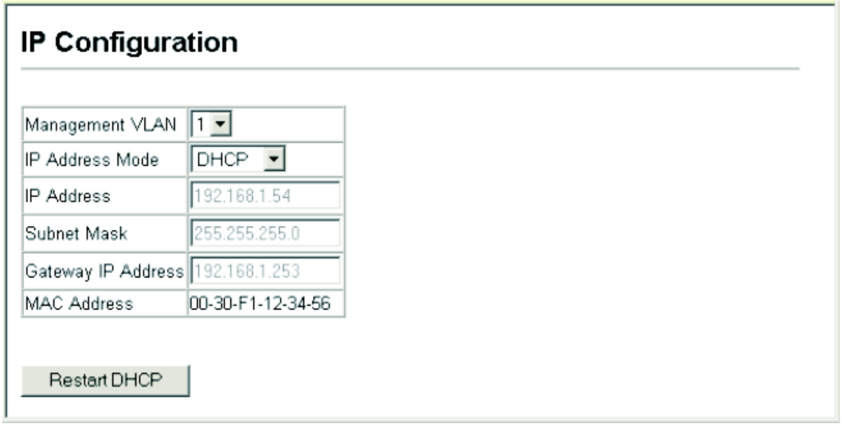
CLI – Specify the management interface, IP address and default gateway.

```
Console#config
Console(config)#interface vlan 1                                      4-86
Console(config-if)#ip address 192.168.1.254 255.255.255.0             4-165
Console(config-if)#exit
Console(config)#ip default-gateway 192.168.1.253                      4-166
Console(config)#
```

Using DHCP/BOOTP

If your network provides DHCP/BOOTP services, you can configure the switch to be dynamically configured by these services.

Web – Click System, IP Configuration. Specify the VLAN to which the management station is attached, set the IP Address Mode to DHCP or BOOTP. Click Apply to save your changes. Then click Restart DHCP to immediately request a new address. Note that the switch will also broadcast a request for IP configuration settings on each power reset.



IP Configuration

Management VLAN	1
IP Address Mode	DHCP
IP Address	192.168.1.54
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.253
MAC Address	00-30-F1-12-34-56

Note: If you lose your management connection, use a console connection and enter “show ip interface” to determine the new switch address.

CLI – Specify the management interface, and set the IP address mode to DHCP or BOOTP, and then enter the **ip dhcp restart** command.

```
Console#config
Console(config)#interface vlan 1                                      4-86
Console(config-if)#ip address dhcp                                    4-165
Console(config-if)#end
Console#ip dhcp restart                                               4-85
Console#show ip interface                                             4-166
 IP address and netmask: 192.168.1.54 255.255.255.0 on VLAN 1,
 and address mode: DHCP.
Console#
```

Renewing DCHP – DHCP may lease addresses to clients indefinitely or for a specific period of time. If the address expires or the switch is moved to another network segment, you will lose management access to the switch. In this case, you can reboot the switch or submit a client request to restart DHCP service via the CLI.

Web – If the address assigned by DHCP is no longer functioning, you will not be able to renew the IP settings via the web interface. You can only restart DHCP service via the web interface if the current address is still available.

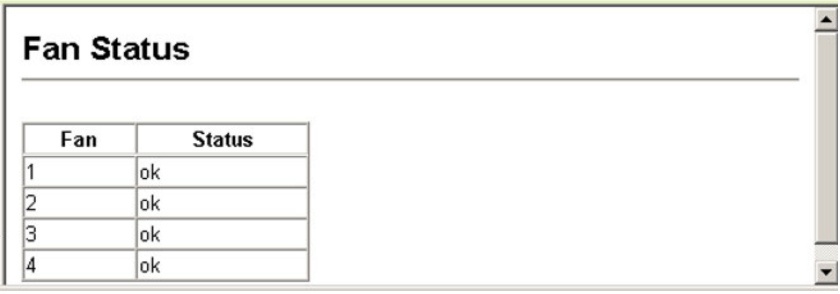
CLI – Enter the following command to restart DHCP service.

```
Console#ip dhcp restart                                          4-85
Console#
```

Fan Status

The status of the switch fans can be displayed.

Web – Click System, Fan Status.



Fan Status

Fan	Status
1	ok
2	ok
3	ok
4	ok

Managing Firmware

You can upload/download firmware to or from a TFTP server. By saving runtime code to a file on a TFTP server, that file can later be downloaded to the switch to restore operation. You can also set the switch to use new firmware without overwriting the previous version. The drop down menu in the web interface allows you to specify the method of file transfer.

Command Attributes

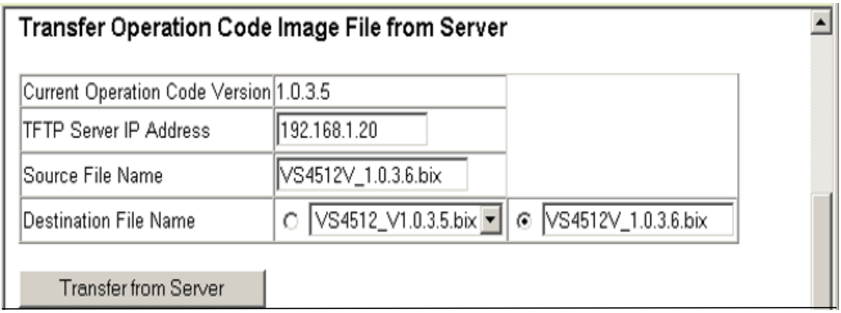
- **TFTP Server IP Address** – The IP address of a TFTP server.
- **File Name** – The file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”)
- **Destination/Startup File Name** – Allows specification of filenames already in memory, or the creation of a new filename. (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”)
- **Source File Name** – Allows you to specify the name of the chosen source file.

Note: Up to two copies of the system software (i.e., the runtime firmware) can be stored in the file directory on the switch. The currently designated startup version of this file cannot be deleted.

Downloading System Software from a Server

When downloading runtime code, you can specify the destination file name to replace the current image, or first download the file using a different name from the current runtime code file, and then set the new file as the startup file.

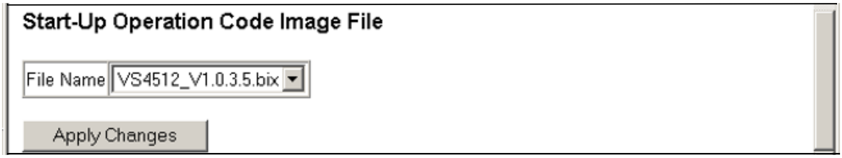
Web – Click System, Firmware. Enter the source and destination file names with any other relevent details such as the IP address of the TFTP server if used, and click Transfer from Server.



Transfer Operation Code Image File from Server

Current Operation Code Version	1.0.3.5	
TFTP Server IP Address	192.168.1.20	
Source File Name	VS4512V_1.0.3.6.bix	
Destination File Name	○ VS4512_V1.0.3.5.bix ▼	● VS4512V_1.0.3.6.bix

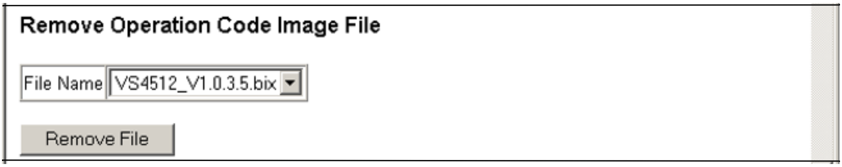
If you download to a new destination file, then select the file from the drop-down box for the operation code used at startup, and click Apply Changes. To start the new firmware, reboot the system via the System/Reset menu.



Start-Up Operation Code Image File

File Name: VS4512_V1.0.3.5.bix ▼

To remove an operating code file, select the file from the drop-down list and click Remove File.



Remove Operation Code Image File

File Name: VS4512_V1.0.3.5.bix ▼

CLI – Enter the IP address of the TFTP server, select “config” or “opcode” file type, then enter the source and destination file names, set the new file to start up the system, and then restart the switch.

```
Console#copy tftp file                                                   4-57
TFTP server ip address: 10.1.0.19
Choose file type:
 1. config:  2. opcode: <1-2>: 2
Source file name: M100000.bix
Destination file name: V1.0
\Write to FLASH Programming.
-Write to FLASH finish.
Success.
Console#config
Console(config)#boot system opcode:V1.0                                  4-61
Console(config)#exit
Console#reload                                                           4-21
```

Saving or Restoring Configuration Settings

You can upload/download configuration settings to/from a TFTP server. The configuration file can be later downloaded to restore the switch’s settings.

Command Attributes

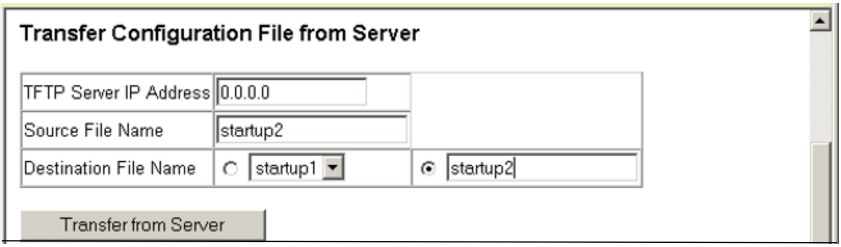
- **TFTP Server IP Address** – The IP address of a TFTP server.
- **File Name** – The configuration file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”)

Note: The maximum number of user-defined configuration files is limited only by available flash memory space.

Downloading Configuration Settings from a Server

You can download the configuration file under a new file name and then set it as the startup file, or you can specify the current startup configuration file as the destination file to directly replace it. Note that the file “Factory_Default_Config.cfg” can be copied to the TFTP server, but cannot be used as the destination on the switch.

Web – Click System, Configuration. Enter the IP address of the TFTP server, enter the name of the file to download, select a file on the switch to overwrite or specify a new file name, and then click Transfer from Server.

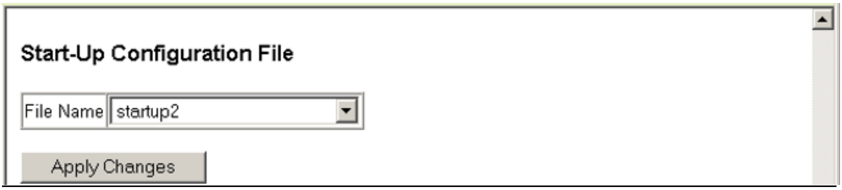


Transfer Configuration File from Server

TFTP Server IP Address	0.0.0.0	
Source File Name	startup2	
Destination File Name	○ startup1 ▼	● startup2

Setting the Startup Configuration File

If you download to a new file name, select the new file from the drop-down list for Startup Configuration File, and press Apply Changes. To use the new settings, reboot the system via the System/Reset menu.



Start-Up Configuration File

File Name: startup2

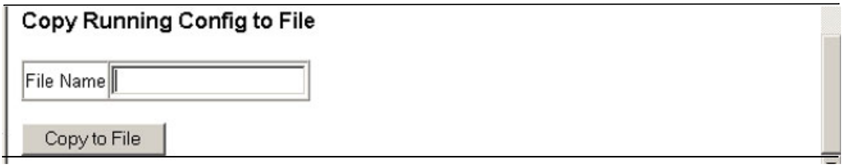
CLI – Enter the IP address of the TFTP server, specify the source file on the server, set the startup file name on the switch, and then restart the switch.

```
Console#copy tftp startup-config                                          4-57
TFTP server ip address: 192.168.1.19
Source configuration file name: config-1
Startup configuration file name [] : startup
\Write to FLASH Programming.
-Write to FLASH finish.
Success.

Console#reload
```

Copying the Running Configuration to a File

You can copy the running configuration to a file.



Copy Running Config to File

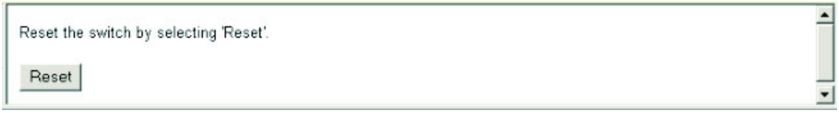
File Name:

If you download the startup configuration file under a new file name, you can set this file as the startup file at a later time, and then restart the switch.

```
Console#copy tftp startup-config                                          4-57
TFTP server ip address: 192.168.1.19
Source configuration file name: startup2.0
Startup configuration file name [startup] : startup2.0
/
Console#config
Console(config)#boot system config: startup-new                          4-61
Console(config)#exit
Console#reload                                                            4-21
```

Resetting the System

Web – Click System, Reset. Click the Reset button to restart the switch.



Reset the switch by selecting 'Reset'.

CLI – Use the reload command to restart the switch.

```
Console#reload                                                4-21
System will be restarted, continue <y/n>?
```

Note: When restarting the system, it will always run the Power-On Self-Test.

Setting the System Clock

Simple Network Time Protocol (SNTP) allows the switch to set its internal clock based on periodic updates from a time server (SNTP or NTP). Maintaining an accurate time on the switch enables the system log to record meaningful dates and times for event entries. You can also manually set the clock using the CLI. (See “calendar set” on page 49.) If the clock is not set, the switch will only record the time from the factory default set at the last bootup.

This switch acts as an SNTP client in two modes:

Unicast – The switch periodically sends a request for a time update to a configured time server. You can configure up to three time server IP addresses. The switch will attempt to poll each server in the configured sequence.

Broadcast – The switch sets its clock from a time server in the same subnet that broadcasts time updates. If there is more than one SNTP server, the switch accepts the first broadcast it detects and ignores broadcasts from other servers.

Configuring SNTP

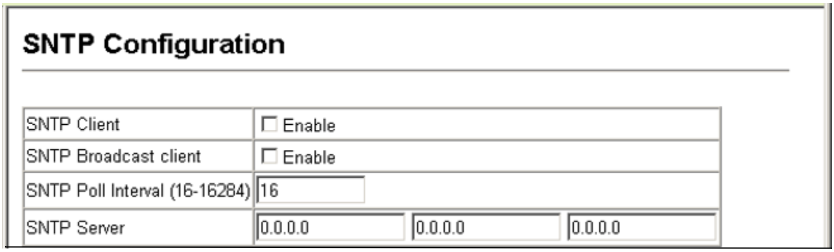
You can configure the switch to send time synchronization requests to specific time servers (i.e., client mode), update its clock using information broadcast from time servers, or use both methods. When both methods are enabled, the switch will update its clock using information broadcast from time servers, but will query the specified server(s) if a broadcast is not received within the polling interval.

Command Attributes

- **SNTP Client** – Configures the switch to operate as an SNTP unicast client. This mode requires at least one time server to be specified in the SNTP Server field.
- **SNTP Broadcast Client** – Configures the switch to operate as an SNTP broadcast client.

- **SNTP Poll Interval** – Sets the interval between sending requests for a time update from a time server when set to SNTP Client mode.
 (Range: 16-16284 seconds; Default: 16 seconds)
- **SNTP Server** – In unicast mode, sets the IP address for up to three time servers. The switch attempts to update the time from the first server, if this fails it attempts an update from the next server in the sequence.

Web – Select SNTP, Configuration. Modify any of the required parameters, and click Apply.



SNTP Configuration

SNTP Client	□ Enable		
SNTP Broadcast client	□ Enable		
SNTP Poll Interval (16-16284)	16		
SNTP Server	0.0.0.0	0.0.0.0	0.0.0.0

CLI – This example configures the switch to operate as an SNTP client and as an SNTP broadcast client.

```
Console(config)#sntp client                                              4-45
Console(config)#sntp poll 16                                             4-47
Console(config)#sntp server 10.1.0.19 137.82.140.80 128.250.36.2         4-46
Console(config)#sntp broadcast client                                    4-48
Console(config)#
```

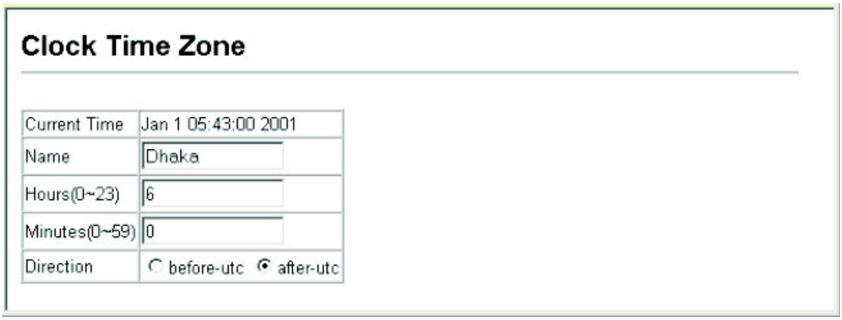
Setting the Time Zone

SNTP uses Coordinated Universal Time (or UTC, formerly Greenwich Mean Time, or GMT) based on the time at the Earth’s prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is east (before) or west (after) of UTC.

Command Attributes

- **Current Time** – Displays the current time.
- **Name** – Assigns a name to the time zone.
- **Hours (0-12)** – The number of hours before/after UTC.
- **Minutes (0-59)** – The number of minutes before/after UTC.
- **Direction** – Configures the time zone to be before (east) or after (west) UTC.

Web – Select SNTP, Clock Time Zone. Set the offset for your time zone relative to the UTC, and click Apply.



Clock Time Zone

Current Time	Jan 1 05:43:00 2001
Name	Dhaka
Hours(0~23)	6
Minutes(0~59)	0
Direction	○ before-utc ● after-utc

CLI - This example shows how to set the time zone for the system clock.

```
Console(config)#clock timezone Dhaka hours 6 minute 0 after-UTC      4-49
Console#
```

Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is a communication protocol designed specifically for managing devices on a network. Equipment commonly managed with SNMP includes switches, routers and host computers. SNMP is typically used to configure these devices for proper operation in a network environment, as well as to monitor them to evaluate performance or detect potential problems.

The switch includes an onboard SNMP agent that continuously monitors the status of its hardware, as well as the traffic passing through its ports. A network management station can access this information using software such as AccView. Access rights to the onboard agent are controlled by community strings. To communicate with the switch, the management station must first submit a valid community string for authentication. The options for configuring community strings, trap functions, and restricting access to clients with specified IP addresses are described in the following sections.

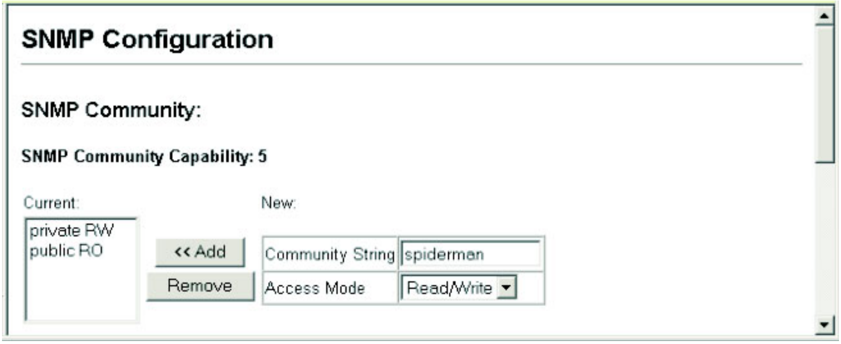
Setting Community Access Strings

You may configure up to five community strings authorized for management access. All community strings used for IP Trap Managers should be listed in this table. For security reasons, you should consider removing the default strings.

Command Attributes

- **SNMP Community Capability** – Indicates that the switch supports up to five community strings.
- **Community String** – A community string that acts like a password and permits access to the SNMP protocol.
  Default strings: "public" (read-only access), "private" (read/write access)
  Range: 1-32 characters, case sensitive
- **Access Mode**
  - **Read-Only** – Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
  - **Read/Write** – Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects.

Web – Click SNMP, Configuration. Add new community strings as required, select the access rights from the Access Mode drop-down list, then click Add.



SNMP Configuration

SNMP Community:

SNMP Community Capability: 5

Current:

private RW
public RO

New:

Community String: spiderman
Access Mode: Read/Write

CLI – The following example adds the string "spiderman" with read/write access.

```
Console(config)#snmp-server community spiderman rw                  4-78
Console(config)#
```

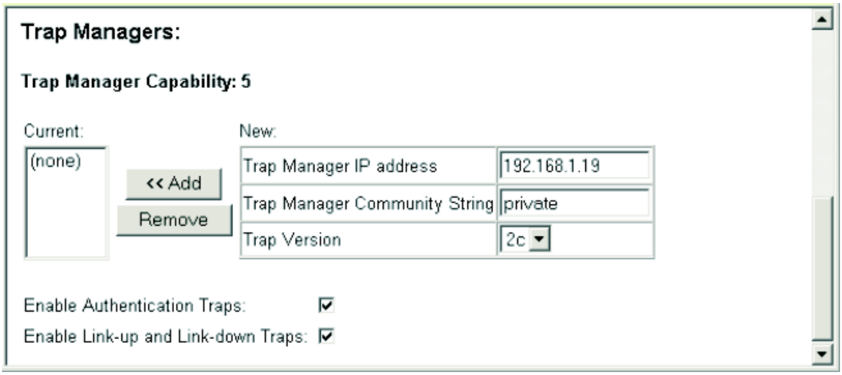
Specifying Trap Managers and Trap Types

Traps indicating status changes are issued by the switch to specified trap managers. You must specify trap managers so that key events are reported by this switch to your management station (using network management platforms such as HP OpenView. You can specify up to five management stations that will receive authentication failure messages and other trap messages from the switch.

Command Attributes

- **Trap Manager Capability** – This switch supports up to five trap managers.
- **Trap Manager IP Address** – Internet address of the host (the targeted recipient).
- **Trap Manager Community String** – Community string sent with the notification operation. (Range: 1-32 characters, case sensitive)
- **Trap Version** – Specifies whether to send notifications as SNMP v1 or v2c traps. (The default is version 1.)
- **Enable Authentication Traps** – Issues a trap message whenever an invalid community string is submitted during the SNMP access authentication process. (The default is enabled.)
- **Enable Link-up and Link-down Traps** – Issues link-up or link-down traps. (The default is enabled.)

Web – Click SNMP, Configuration. Fill in the IP address and community string for each trap manager that will receive these messages, specify the SNMP version, mark the trap types required, and then click Add.



Trap Managers:

Trap Manager Capability: 5

Current: (none)

New:

Trap Manager IP address	192.168.1.19
Trap Manager Community String	private
Trap Version	2c

Enable Authentication Traps: ☑

Enable Link-up and Link-down Traps: ☑

CLI – This example adds a trap manager and enables both authentication and link-up, link-down traps.

```
Console(config)#snmp-server host 192.168.1.19 private version 2c     4-80
Console(config)#snmp-server enable traps                             4-81
```

Filtering Addresses for SNMP Client Access

The switch allows you to create a list of up to 16 IP addresses or IP address groups that are allowed access to the switch via SNMP management software.

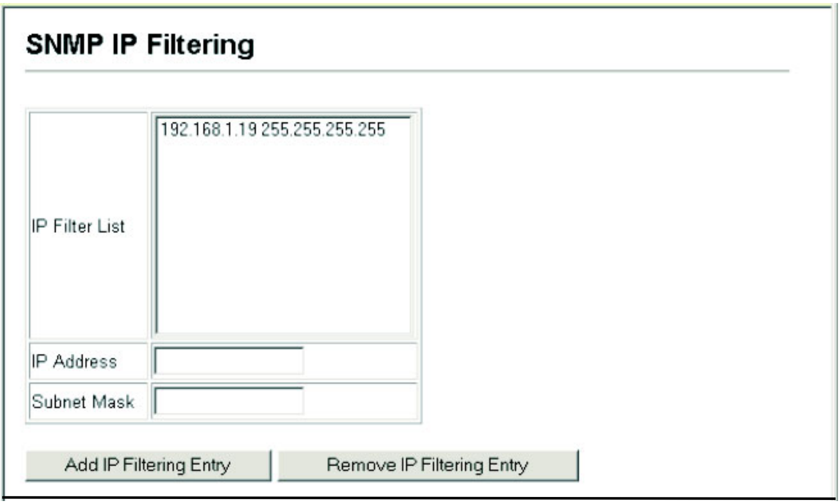
Command Usage

- To specify the clients allowed SNMP access, enter an IP address along with a subnet mask to identify a specific host or a range of valid addresses. For example:
  - IP address 192.168.1.1 and mask 255.255.255.255 –
    Specifies a valid IP address of 192.168.1.1 for a single client.
  - IP address 192.168.1.1 and mask 255.255.255.0 –
    Specifies a valid IP address group from 192.168.1.0 to 192.168.1.254.
- IP filtering only restricts management access for clients running SNMP management software such as AccView. It does not affect management access to the switch using the web interface or Telnet.
- The default setting is null, which allows all IP groups SNMP access to the switch. If one or more IP addresses are configured, IP filtering is enabled and only addresses listed in this table will have SNMP access.

Command Attributes

- **IP Filter List** – Displays a list of the IP address/subnet mask entries currently configured for SNMP access.
- **IP address** – Specifies a new IP address to add to the IP Filter List.
- **Subnet Mask** – Specifies a single IP address or group of addresses. If the IP is the address of a single management station, set the mask to 255.255.255.255. Otherwise, an IP address group will be specified by any other mask.

Web – Click SNMP, IP Filtering. To add a client, enter the new address, the subnet mask for a node or an address range, and then click “Add IP Filtering Entry.”



SNMP IP Filtering

IP Filter List	192.168.1.19 255.255.255.255
IP Address	
Subnet Mask	

CLI – This example allows SNMP access for a specific client.

```
Console(config)#snmp ip filter 10.1.2.3 255.255.255.255            4-82
Console(config)#
```

User Authentication.

Use the Passwords or RADIUS/TACACS+ menu to restrict management access based on specified user names and passwords. You can manually configure access rights on the switch (Passwords menu), or you can use a remote access authentication server based on the RADIUS/TACACS+ protocol. You can also use IEEE 802.1x port authentication to control access to specific ports (dot1X menu).

Configuring the Logon Password

The guest only has read access for most configuration parameters. However, the administrator has write access for all parameters governing the onboard agent. You should therefore assign a new administrator password as soon as possible, and store it in a safe place.

The default guest name is “guest” with the password “guest.” The default administrator name is “admin” with the password “admin.” Note that user names can only be assigned via the CLI.

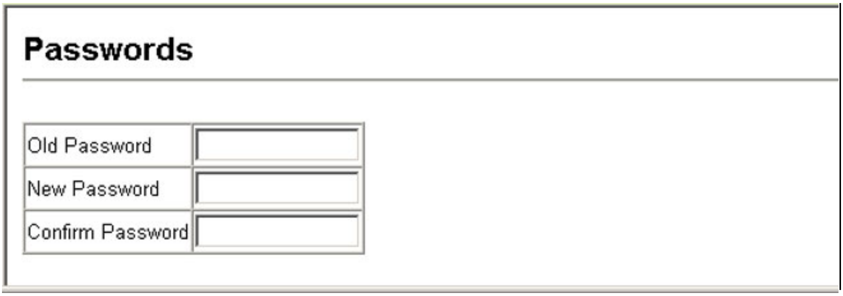
Command Attributes

- **User Name*** – The name of the user.
  (Maximum length: 8 characters; maximum number of users: 5)

- **Access Level*** – Specifies the user level.
  (Options: Normal and Privileged)
- **Password** – Specifies the user password.
  (Range: 0-8 characters plain text, case sensitive)

* CLI only.

Web – Click System, Passwords. Enter the old password, enter the new password, confirm it by entering it again, then click Apply.



Passwords

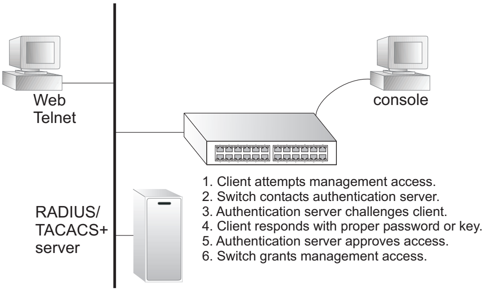
Old Password	
New Password	
Confirm Password	

CLI – Assign a user name to access-level 15 (i.e., administrator), then specify the password.

```
Console(config)#username bob access-level 15                    4-24
Console(config)#username bob password 0 smith
Console(config)#
```

Configuring Local/Remote Logon Authentication

Use the Authentication Settings menu to restrict management access based on specified user names and passwords. You can manually configure access rights on the switch, or you can use a remote access authentication server based on RADIUS or TACACS+ protocols.



1. Client attempts management access.
2. Switch contacts authentication server.
3. Authentication server challenges client.
4. Client responds with proper password or key.
5. Authentication server approves access.
6. Switch grants management access.

Remote Authentication Dial-in User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+) are logon authentication protocols that use software running on a central server to control access to RADIUS-aware or TACACS -aware devices on the network. An authentication server contains a database of multiple user name/ password pairs with associated privilege levels for each user that requires management access to the switch.

RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.

Command Usage

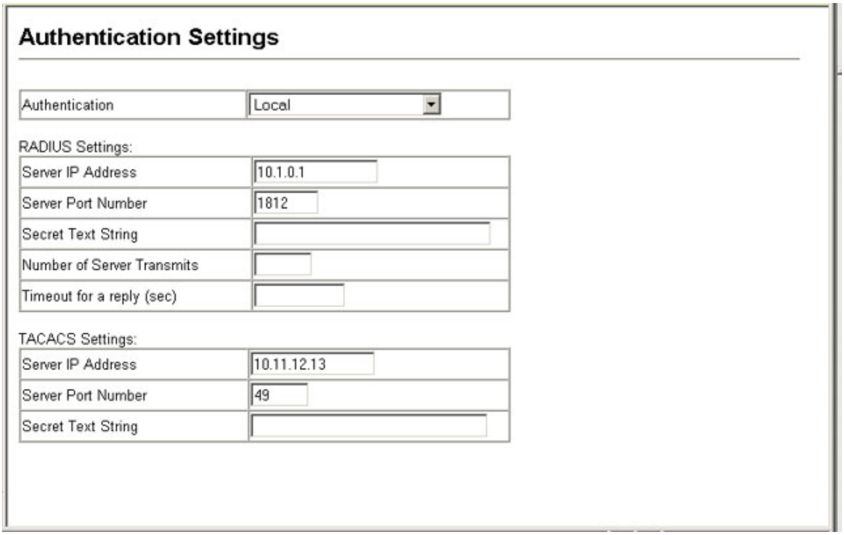
- By default, management access is always checked against the authentication database stored on the local switch. If a remote authentication server is used, you must specify the authentication sequence and the corresponding parameters for the remote authentication protocol. Local and remote logon authentication control management access via the console port, web browser, or Telnet.
- RADIUS and TACACS+ logon authentication assign a specific privilege level for each user name/password pair. The user name, password, and privilege level must be configured on the authentication server.
- You can specify up to three authentication methods for any user to indicate the authentication sequence. For example, if you select (1) RADIUS, (2) TACACS and (3) Local, the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted using the TACACS+ server, and finally the local user name and password is checked.

Command Attributes

- **Authentication** – Select the authentication, or authentication sequence required:
  - **Local** – User authentication is performed only locally by the switch.
  - **Radius** – User authentication is performed using a RADIUS server only.
  - **TACACS** – User authentication is performed using a TACACS+ server only.
  - [authentication sequence] – User authentication is performed by up to three authentication methods in the indicated sequence.
- **RADIUS Settings**
  - **Server IP Address** – Address of authentication server. (Default: 10.1.0.1)
  - **Server Port Number** – Network (UDP) port of authentication server used for authentication messages. (Range: 1-65535; Default: 1812)
  - **Secret Text String** – Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 20 characters)
  - **Number of Server Transmits** – Number of times the switch tries to authenticate logon access via the authentication server.
    (Range: 1-30; Default: 2)
  - **Timeout for a reply** – The number of seconds the switch waits for a reply from the RADIUS server before it resends the request.
    (Range: 1-65535; Default: 5)
- **TACACS Settings**
  - **Server IP Address** – Address of the TACACS+ server. (Default: 10.11.12.13)
  - **Server Port Number** – Network (TCP) port of TACACS+ server used for authentication messages. (Range: 1-65535; Default: 49)
  - **Secret Text String** – Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 20 characters)

Note: The local switch user database has to be set up by manually entering user names and passwords using the CLI. (See “username” on page 24.)

Web – Click Security, Authentication Settings. To configure local or remote authentication preferences, specify the authentication sequence (i.e., one to three methods), fill in the parameters for RADIUS or TACACS+ authentication if selected, and click Apply.



Authentication Settings

Authentication	Local

RADIUS Settings:

Server IP Address	10.1.0.1
Server Port Number	1812
Secret Text String	
Number of Server Transmits	
Timeout for a reply (sec)	

TACACS Settings:

Server IP Address	10.11.12.13
Server Port Number	49
Secret Text String	

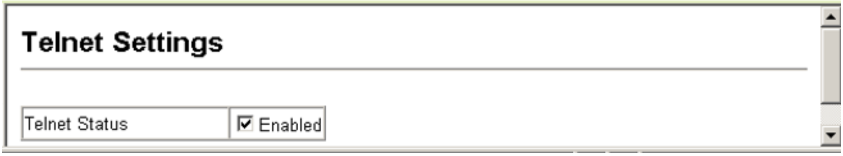
CLI – Specify all the required parameters to enable logon authentication.

```
Console(config)#authentication login radius                           4-62
Console(config)#radius-server host 192.168.1.25                        4-64
Console(config)#radius-server port 181                                 4-64
Console(config)#radius-server key green                                4-65
Console(config)#radius-server retransmit 5                             4-65
Console(config)#radius-server timeout 10                               4-66
Console#show radius-server                                             4-66
Server IP address: 192.168.1.25
 Communication key with radius server:
 Server port number: 181
 Retransmit times: 5
 Request timeout: 10
Console(config)#authentication login tacacs                            4-62
Console(config)#tacacs-server host 10.20.30.40                         4-67
Console(config)#tacacs-server port 200                                 4-67
Console(config)#tacacs-server key green                                4-68
Console#show tacacs-server                                             4-68
Server IP address: 10.20.30.40
 Communication key with tacacs server: green
 Server port number: 200
Console(config)#
```

Telnet Settings

Telnet access to the switch can be enabled via the Web or CLI.

Web – Click Security, Telnet Settings, then check the checkbox to enable access via Telnet (i.e., a virtual terminal).



Telnet Settings

Telnet Status ☑ Enabled

CLI – This example enables Telnet access to the switch.

```
Console#config                                                     4-31
Console(config)#ip telnet server
Console(config-line)#
```

Configuring HTTPS

You can configure the switch to enable the Secure Hypertext Transfer Protocol (HTTPS) over the Secure Socket Layer (SSL), providing secure access (i.e., an encrypted connection) to the switch’s web interface.

Command Usage

- Both the HTTP and HTTPS service can be enabled independently on the switch. However, you cannot configure both services to use the same UDP port.
- If you enable HTTPS, you must indicate this in the URL that you specify in your browser: https://*device*[:*port_number*]
- When you start HTTPS, the connection is established in this way:
  - The client authenticates the server using the server’s digital certificate.
  - The client and server negotiate a set of security protocols to use for the connection.
  - The client and server generate session keys for encrypting and decrypting data.
- The client and server establish a secure encrypted connection.
  A padlock icon should appear in the status bar for Internet Explorer 5.x or above and Netscape Navigator 4.x or above.
- The following web browsers and operating systems currently support HTTPS:

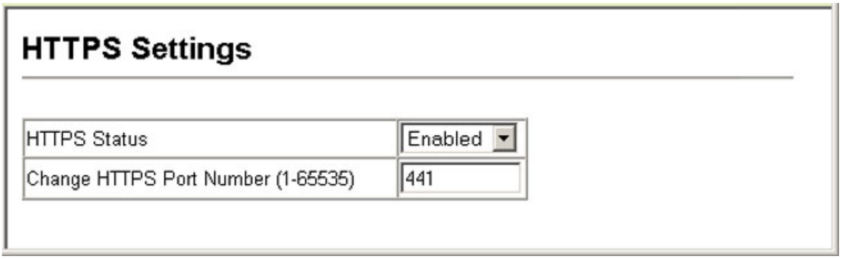
Web Browser	Operating System
Internet Explorer 5.0 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP
Netscape Navigator 4.76 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP, Solaris 2.6

- To specify a secure-site certificate, see “Replacing the Default Secure-site Certificate” on page 3-29.

Command Attributes

- **HTTPS Status** – Allows you to enable/disable the HTTPS server feature on the switch. (Default: Enabled)
- **Change HTTPS Port Number** – Specifies the UDP port number used for HTTPS/SSL connection to the switch's web interface. (Default: Port 443)

Web – Click Security, HTTPS Settings. Enable HTTPS and specify the port number, then click Apply.



HTTPS Settings

HTTPS Status	Enabled
Change HTTPS Port Number (1-65535)	441

CLI – This example enables the HTTP secure server and modifies the port number.

```
Console(config)#ip http secure-server                                     4-29
Console(config)#ip http secure-port 441                                   4-30
Console(config)#
```

Replacing the Default Secure-site Certificate

When you log onto the web interface using HTTPS (for secure access), a Secure Sockets Layer (SSL) certificate appears for the switch. By default, the certificate that Netscape and Internet Explorer display will be associated with a warning that the site is not recognized as a secure site. This is because the certificate has not been signed by an approved certification authority. If you want this warning to be replaced by a message confirming that the connection to the switch is secure, you must obtain a unique certificate and a private key and password from a recognized certification authority.

Caution: For maximum security, we recommend you obtain a unique Secure Sockets Layer certificate at the earliest opportunity. This is because the default certificate for the switch is not unique to the hardware you have purchased.

When you have obtained these, place them on your TFTP server, and use the following command at the switch's command-line interface to replace the default (unrecognized) certificate with an authorized one:

```
Console#copy tftp https-certificate                                       4-57
TFTP server ip address: <server ip-address>
Source certificate file name: <certificate file name>
Source private file name: <private key file name>
Private password: <password for private key>
```

Note: The switch must be reset for the new certificate to be activated. To reset the switch, type: `Console#reload`

Configuring the Secure Shell

The Berkley-standard includes remote access tools originally designed for Unix systems. Some of these tools have also been implemented for Microsoft Windows and other environments. These tools, including commands such as, *rsh* (remote shell), and *rexec* (remote execute), are not secure from hostile attacks.

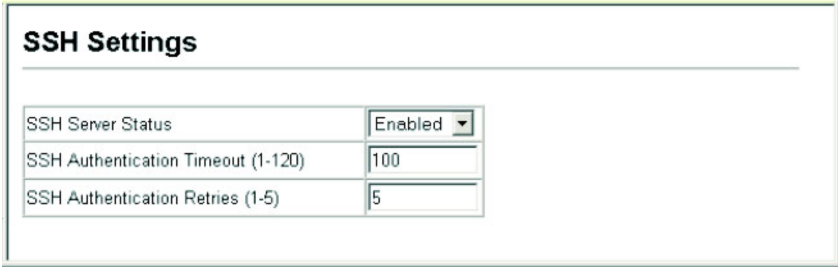
The Secure Shell (SSH) includes server/client applications intended as a secure replacement for the older Berkley remote access tools. SSH provides remote management access via encrypted paths between the switch and SSH-enabled management station clients. The commands described in this section include commands used to configure the SSH server. However, you also need to install a SSH client on the management station when using this protocol to configure the switch. When the client contacts the switch via the SSH protocol, the switch generates a public-key that the client uses along with a local user name and password for access authentication.

Note: The switch supports only SSH Version 1.5.

Command Attributes

- **SSH Server Status** – Allows you to enable/disable the SSH server feature on the switch. (Default: Enabled)
- **SSH Authentication Timeout** – Specifies the time interval in seconds that the SSH server waits for a response from a client during an authentication attempt.
- (Range: 1 to 120 seconds; Default: 120 seconds)
- **SSH Authentication Retries** – Specifies the number of authentication attempts that a client is allowed before authentication fails and the client has to restart the authentication process. (Range: 1-5 times; Default: 3)

Web – Click Security, SSH, Settings. Enable SSH and adjust the authentication parameters as required, then click Apply.



SSH Settings

SSH Server Status	Enabled
SSH Authentication Timeout (1-120)	100
SSH Authentication Retries (1-5)	5

CLI – This example enables SSH, sets the authentication parameters, and displays the current configuration. It shows that the administrator has made a connection via SHH, and then disabled this connection.

```
Console(config)#ip ssh server                                        4-32
Console(config)#ip ssh timeout 100                                   4-35
Console(config)#ip ssh authentication-retries 5                      4-33
Console(config)#
Console#show ip ssh                                                  4-34
Information of secure shell
SSH status: enable
SSH authentication timeout: 100
SSH authentication retries: 5
Console#show ssh                                                     4-35
Information of secure shell
Session Username Version Encrypt method Negotiation state
------- -------- ------- ------------- -----------------
      0    admin   1.5      cipher-3des   session-started
Console#disconnect ssh 0                                             4-16
Console#
```

Configuring Port Security

Port security is a feature that allows you to configure a switch port with one or more device MAC addresses that are authorized to access the network through that port.

When port security is enabled on a port, the switch stops learning new MAC addresses on the specified port. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted as authorized to access the network through that port. If a device with an unauthorized MAC address attempts to use the switch port, the intrusion will be detected and the switch can automatically take action by disabling the port and sending a trap message.

To use port security, first allow the switch to dynamically learn the <source MAC address, VLAN> pair for frames received on a port for an initial training period, and then enable port security to stop address learning. Be sure you enable the learning function long enough to ensure that all valid VLAN members have been registered on the selected port. Note that you can also restrict the maximum number of addresses that can be learned by a port.

To add new VLAN members at a later time, you can manually add secure addresses with the Static Address Table (page 3-70), or turn off port security to reenable the learning function long enough for new VLAN members to be registered. Learning may then be disabled again, if desired, for security.

Command Usage

- A secure port has the following restrictions:
  - It cannot use port monitoring.
  - It cannot be a multi-VLAN port.
  - It cannot be used as a member of a static or dynamic trunk.
  - It should not be connected to a network interconnection device.
- If a port is disabled (shut down) due to a security violation, it must be manually re-enabled from the Port/Port Configuration page (page 3-42).

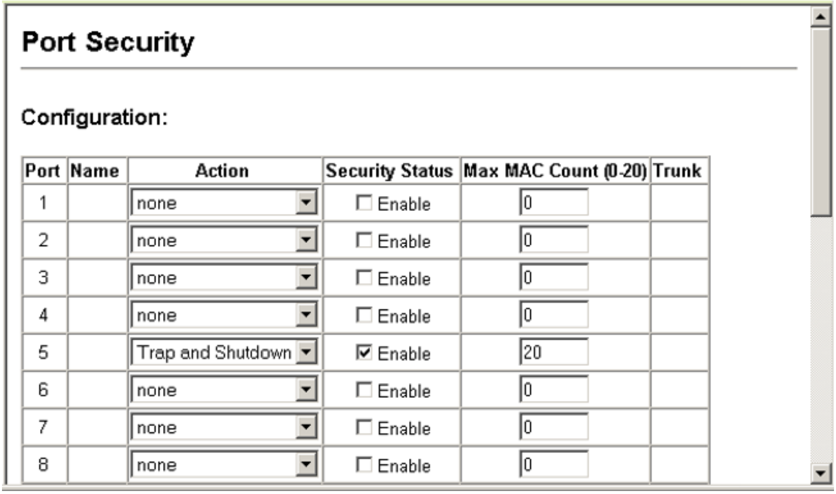
Command Attributes

- **Port** – Port number.
- **Action*** – The action to be taken when a port security violation is detected:
  - **None**: No action should be taken. (This is the default.)
  - **Trap**: Send an SNMP trap message.
  - **Shutdown**: Disable the port.
  - **Trap and Shutdown**: Send an SNMP trap message and disable the port.

* These actions can only be taken through CLI commands.

- **Status** – Enables or disables port security on the port. (Default: Disabled)
- **Max MAC Count** – The maximum number of MAC addresses that can be learned on a port. (Range: 0 - 20)

Web – Click Security, Port Security. Set the action to take when an invalid address is detected on a port, select Enabled from the drop-down list in the Status column to enable security for a port, set the maximum number of MAC addresses allowed on a port, and click Apply.



Port Security

Configuration:

Port	Name	Action	Security Status	Max MAC Count (0-20)	Trunk
1		none	□ Enable	0	
2		none	□ Enable	0	
3		none	□ Enable	0	
4		none	□ Enable	0	
5		Trap and Shutdown	☑ Enable	20	
6		none	□ Enable	0	
7		none	□ Enable	0	
8		none	□ Enable	0	

CLI – This example sets the command mode to Port 5, sets the port security action to send a trap and disable the port, and then enables port security for the switch.

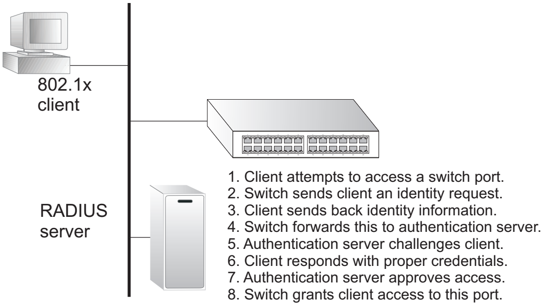
```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap-and-shutdown          4-69
Console(config-if)#port security
Console(config-if)#
```

Configuring 802.1x Port Authentication

Network switches can provide open and easy access to network resources by simply attaching a client PC. Although this automatic configuration and access is a desirable feature, it also allows unauthorized personnel to easily intrude and possibly gain access to sensitive network data.

The IEEE 802.1x (dot1x) standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. Access to all switch ports in a network can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

This switch uses the Extensible Authentication Protocol over LANs (EAPOL) to exchange authentication protocol messages with the client, and a remote RADIUS authentication server to verify user identity and access rights. When a client (i.e., Supplicant) connects to a switch port, the switch (i.e., Authenticator) responds with an EAPOL identity request. The client provides its identity (such as a user name) in an EAPOL response to the switch, which it forwards to the RADIUS server. The RADIUS server verifies the client identity and sends an access challenge back to the client. The EAP packet from the RADIUS server contains not only the challenge, but the authentication method to be used. The client can reject the authentication method and request another, depending on the configuration of the client software and the RADIUS server. The authentication method can be MD5, TLS (Transport Layer Security), TTLS (Tunneled Transport Layer Security), or other. The client responds to the appropriate method with its credentials, such as a password or certificate. The RADIUS server verifies the client credentials and responds with an accept or reject packet. If authentication is successful, the switch allows the client to access the network. Otherwise, network access is denied and the port remains blocked.



1. Client attempts to access a switch port.
2. Switch sends client an identity request.
3. Client sends back identity information.
4. Switch forwards this to authentication server.
5. Authentication server challenges client.
6. Client responds with proper credentials.
7. Authentication server approves access.
8. Switch grants client access to this port.

The operation of 802.1x on the switch requires the following:

- The switch must have an IP address assigned.
- RADIUS authentication must be enabled on the switch and the IP address of the RADIUS server specified.
- Each switch port that will be used must be set to dot1x “Auto” mode.
- Each client that needs to be authenticated must have dot1x client software installed and properly configured.
- The RADIUS server and 802.1x client support EAP. (The switch only supports EAPOL in order to pass the EAP packets from the server to the client.)
- The RADIUS server and client also have to support the same EAP authentication type – MD5, TLS, TTLS, PEAP, etc. (Some clients have native support in Windows, otherwise the dot1x client must support it.)

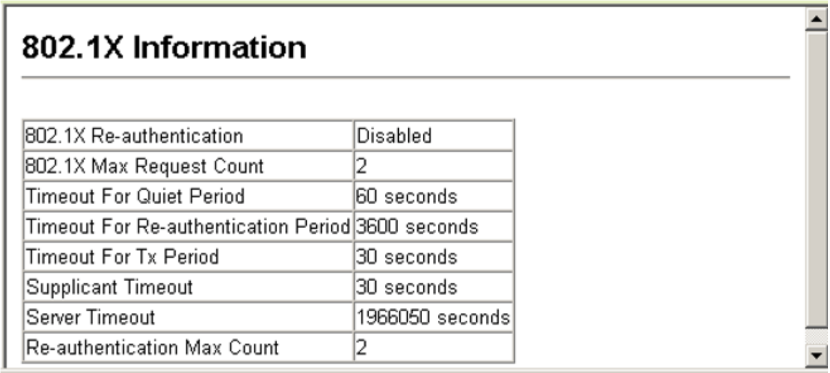
Displaying 802.1x Global Settings

The dot1x protocol includes global parameters that control the client authentication process that runs between the client and the switch (i.e., authenticator), as well as the client identity lookup process that runs between the switch and authentication server. These parameters are described in this section.

Command Attributes

- **802.1x Re-authentication** – Indicates if switch port requires a client to be re-authenticated after a certain period of time.
- **802.1x Max Request Count** – The maximum number of times the switch port will retransmit an EAP request packet to the client before it times out the authentication session.
- **Timeout for Quiet Period** – Indicates the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client.
- **Timeout for Re-authentication Period** – Indicates the time period after which a connected client must be re-authenticated.
- **Timeout for TX Period** – The time period during an authentication session that the switch waits before re-transmitting an EAP packet.
- **Supplicant timeout** – The time the switch waits for a client response to an EAP request.
- **Server timeout** – The time the switch waits for a response from the authentication server (RADIUS) to an authentication request.
- **Re-authentication Max Count** – The number of times the switch will attempt to re-authenticate a connected client before the port becomes unauthorized.

Web – Click Security, 802.1x, Information.



802.1X Information

802.1X Re-authentication	Disabled
802.1X Max Request Count	2
Timeout For Quiet Period	60 seconds
Timeout For Re-authentication Period	3600 seconds
Timeout For Tx Period	30 seconds
Supplicant Timeout	30 seconds
Server Timeout	1966050 seconds
Re-authentication Max Count	2

CLI – This example shows the default protocol settings for 802.1x. For a description of the additional entries displayed in the CLI, See “show dot1x” on page 76.

```
Console#show dot1x                                                   4-76
Global 802.1X Parameters
 reauth-enabled: yes
 reauth-period:  300
 quiet-period:   350
 tx-period:      300
 supp-timeout:   30
 server-timeout: 30
 reauth-max:     2
 max-req:        2

802.1X Port Summary
 Port Name     Status    Operation Mode                Mode     Authorized
       1/1  disabled        Single-Host      ForceAuthorized           n/a
       1/2  disabled        Single-Host      ForceAuthorized           n/a
:
      1/11  disabled        Single-Host      ForceAuthorized           yes
      1/12   enabled        Single-Host                  Auto          yes

802.1X Port Details

802.1X is disabled on port 1
:
802.1X is enabled on port 12
Status              Unauthorized
Operation mode      Single-Host
Max count           5
Port-control        Auto
Supplicant          00-00-00-00-00-00
Current Identifier  0

Authenticator State Machine
State               Connecting
Reauth Count        3

Backend State Machine
State               Idle
Request Count       0
Identifier(Server)  0

Reauthentication State Machine
State               Initialize
Console#
```

Configuring 802.1x Global Settings

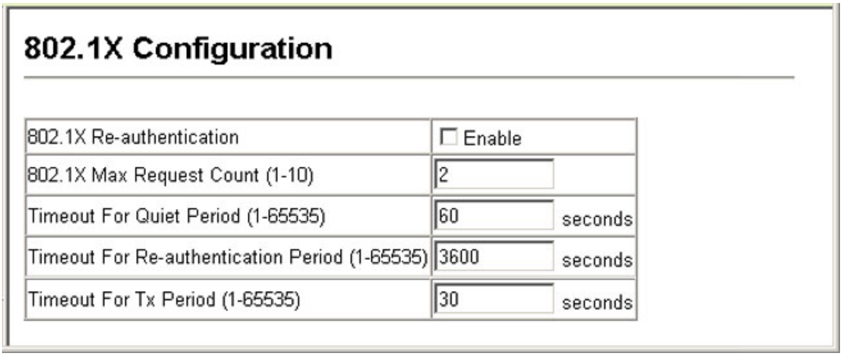
The dot1x protocol includes global parameters that control the client authentication process that runs between the client and the switch (i.e., authenticator), as well as the client identity lookup process that runs between the switch and authentication server. The configuration options for parameters are described in this section.

Command Attributes

- **802.1x Re-authentication** – Sets the client to be re-authenticated after the interval specified by the Timeout for Re-authentication Period. Re-authentication can be used to detect if a new device is plugged into a switch port. (Default: Disabled)
- **802.1x Max Request Count** – Sets the maximum number of times the switch port will retransmit an EAP request packet to the client before it times out the authentication session. (Range: 1-10; Default 2)
- **Timeout for Quiet Period** – Sets the time that a switch port waits after the dot1X Max Request Count has been exceeded before attempting to acquire a new client. (Range: 1-65535 seconds; Default: 60 seconds)
- **Timeout for Re-authentication Period** – Sets the time period after which a connected client must be re-authenticated. (Range: 1-65535 seconds; Default: 3600 seconds)
- **Timeout for TX Period** – Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet. (Range: 1-65535; Default: 30 seconds)
- **authentication dot1x default*** – Sets the default authentication server type. Note that the specified authentication server type must be enabled and properly configured for dot1x to function properly. (Options: radius).

* CLI only.

Web – Select Security, 802.1x, Configuration. Enable dot1x globally for the switch, modify any of the parameters required, and then click Apply.



802.1X Configuration

802.1X Re-authentication	□ Enable
802.1X Max Request Count (1-10)	2
Timeout For Quiet Period (1-65535)	60 seconds
Timeout For Re-authentication Period (1-65535)	3600 seconds
Timeout For Tx Period (1-65535)	30 seconds

CLI – This enables re-authentication and sets all of the global parameters for 802.1x.

```
Console(config)#dot1x re-authentication                             4-74
Console(config)#dot1x max-req 5                                     4-72
Console(config)#dot1x timeout quiet-period 40                       4-74
Console(config)#dot1x timeout re-auth 5                             4-75
Console(config)#dot1x timeout tx-period 40                          4-75
Console(config)#authentication dot1x default radius                 4-71
Console(config)#
```

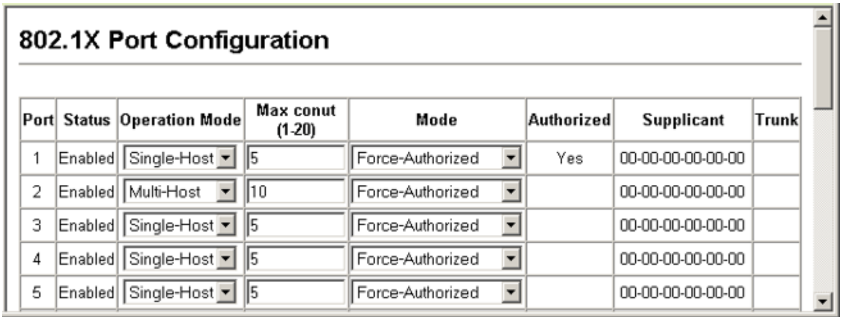
Configuring Port Authorization Mode

When dot1x is enabled, you need to specify the dot1x authentication mode configured for each port.

Command Attributes

- **Status** – Indicates if authentication is enabled or disabled on the port.
- **Operation Mode** – Allows single or multiple hosts (clients) to connect to an 802.1X-authorized port. (Range: Single-Host, Multi-Host; Default: Single-Host)
- **Max Count** – The maximum number of hosts that can connect to a port when the Multi-Host operation mode is selected. (Range: 1-20; Default: 5)
- **Mode** – Sets the authentication mode to one of the following options:
  - **Auto** – Requires a dot1x-aware client to be authorized by the authentication server. Clients that are not dot1x-aware will be denied access.
  - **Force-Authorized** – Forces the port to grant access to all clients, either dot1x-aware or otherwise.
  - **Force-Unauthorized** – Forces the port to deny access to all clients, either dot1x-aware or otherwise.
- **Authorized**
  - **Yes** – Connected client is authorized.
  - **No** – Connected client is not authorized.
  - *Blank* – Displays nothing when dot1x is disabled on a port.
- **Supplicant** – Indicates the MAC address of a connected client.
- **Trunk** – Indicates if the port is configured as a trunk port.

Web – Click Security, 802.1x, Port Configuration. Select the authentication mode from the drop-down box and click Apply.



802.1X Port Configuration

Port	Status	Operation Mode	Max conut (1-20)	Mode	Authorized	Supplicant	Trunk
1	Enabled	Single-Host	5	Force-Authorized	Yes	00-00-00-00-00-00	
2	Enabled	Multi-Host	10	Force-Authorized		00-00-00-00-00-00	
3	Enabled	Single-Host	5	Force-Authorized		00-00-00-00-00-00	
4	Enabled	Single-Host	5	Force-Authorized		00-00-00-00-00-00	
5	Enabled	Single-Host	5	Force-Authorized		00-00-00-00-00-00	

CLI – This example sets the authentication mode to enable 802.1x on port 2, and allows up to ten clients to connect to this port.

```
Console(config)#interface ethernet 1/2                                4-86
Console(config-if)#dot1x port-control auto                            4-72
Console(config-if)#dot1x operation-mode multi-host max-count 10       4-73
Console(config-if)#
```

Displaying 802.1x Statistics

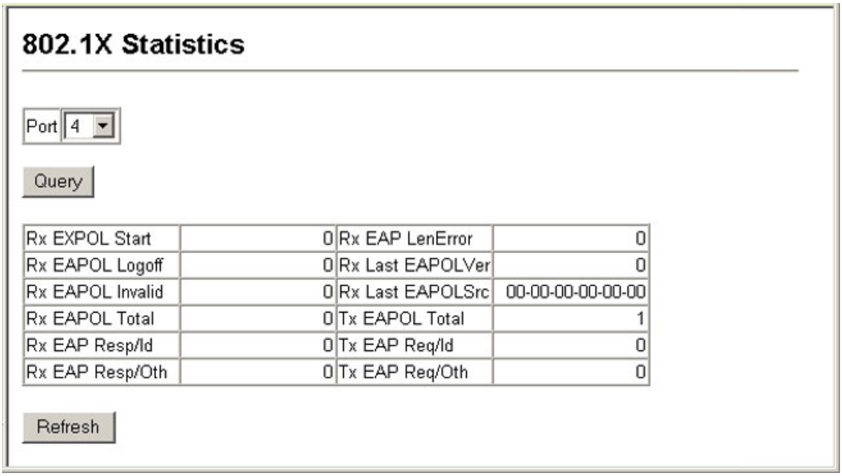
This switch can display statistics for dot1x protocol exchanges for any port.

Statistical Values

Parameter	Description
Rx EXPOL Start	The number of EAPOL Start frames that have been received by this Authenticator.
Rx EAPOL Logoff	The number of EAPOL Logoff frames that have been received by this Authenticator.
Rx EAPOL Invalid	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.
Rx EAPOL Total	The number of valid EAPOL frames of any type that have been received by this Authenticator.
Rx EAP Resp/Id	The number of EAP Resp/Id frames that have been received by this Authenticator.
Rx EAP Resp/Oth	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.
Rx EAP LenError	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
Rx Last EAPOLVer	The protocol version number carried in the most recently received EAPOL frame.
Rx Last EAPOLSrc	The source MAC address carried in the most recently received EAPOL frame.

Parameter	Description
Tx EAPOL Total	The number of EAPOL frames of any type that have been transmitted by this Authenticator.
Tx EAP Req/Id	The number of EAP Req/Id frames that have been transmitted by this Authenticator.
Tx EAP Req/Oth	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.

Web – Select Security, 802.1x, Statistics. Select the required port and then click Query. Click Refresh to update the statistics.



Rx EXPOL Start	0	Rx EAP LenError	0
Rx EAPOL Logoff	0	Rx Last EAPOLVer	0
Rx EAPOL Invalid	0	Rx Last EAPOLSrc	00-00-00-00-00-00
Rx EAPOL Total	0	Tx EAPOL Total	1
Rx EAP Resp/Id	0	Tx EAP Req/Id	0
Rx EAP Resp/Oth	0	Tx EAP Req/Oth	0

CLI – This example displays the 802.1x statistics for port 4.

```
Console#show dot1x statistics interface ethernet 1/4                4-76

Eth 1/4
Rx: EXPOL      EAPOL      EAPOL      EAPOL      EAP      EAP       EAP
    Start      Logoff     Invalid    Total     Resp/Id  Resp/Oth LenError
        2          0          0       1007      672        0         0

    Last       Last
EAPOLVer     EAPOLSrc
       1     00-00-E8-98-73-21

Tx: EAPOL      EAP       EAP
    Total     Req/Id   Req/Oth
     2017     1005        0
Console#
```

Port Configuration

Displaying Connection Status

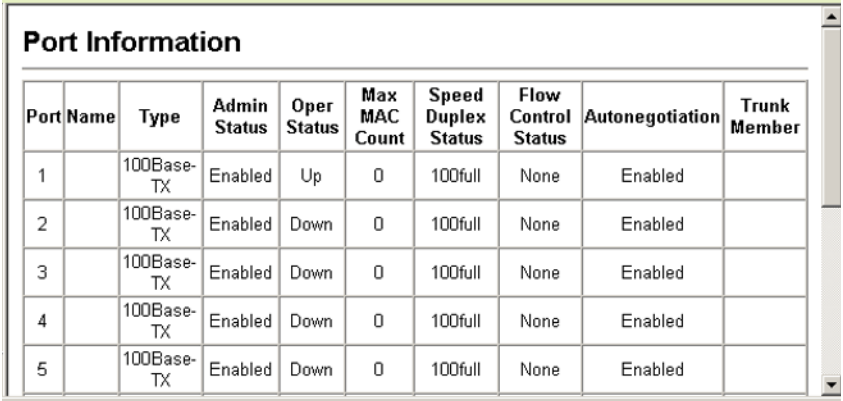
You can use the Port Information or Trunk Information pages to display the current connection status, including link state, speed/duplex mode, flow control, and auto-negotiation.

Field Attributes (Web)

- **Name** – Interface label.
- **Type** – Indicates the port type.
  (1000BASE-T, 1000BASE-SX, 1000BASE-LX, or 100BASE-TX)
- **Admin Status** – Shows if the interface is enabled or disabled.
- **Oper Status** – Indicates if the link is Up or Down.
- Max MAC Count – Shows the maximum number of MAC address that can be learned by a port. (0 - 20 addresses)
- **Speed Duplex Status** – Shows the current speed and duplex mode.
- **Flow Control Status** – Indicates the type of flow control currently in use.
  (IEEE 802.3x, Back-Pressure or None)
- **Autonegotiation** – Shows if auto-negotiation is enabled or disabled.
- **Trunk Member**[1] – Shows if port is a trunk member.
- **Creation**[2] – Shows if a trunk is manually configured or dynamically set via LACP.

1: Port Information only.
2: Trunk Information only

Web – Click Port, Port Information or Trunk Information.



Port Information

Port	Name	Type	Admin Status	Oper Status	Max MAC Count	Speed Duplex Status	Flow Control Status	Autonegotiation	Trunk Member
1		100Base-TX	Enabled	Up	0	100full	None	Enabled	
2		100Base-TX	Enabled	Down	0	100full	None	Enabled	
3		100Base-TX	Enabled	Down	0	100full	None	Enabled	
4		100Base-TX	Enabled	Down	0	100full	None	Enabled	
5		100Base-TX	Enabled	Down	0	100full	None	Enabled	

Command Attributes (CLI)

Basic information:

- **Port type** – Indicates the port type. (1000BASE-T, 1000BASE-SX, 1000BASE-LX, or 100BASE-TX)
- MAC address – The physical layer address for this port. (To access this item on the web, see "Setting the Switch's IP Address" on page 3-11.)

Configuration:

- **Name** – Interface label.
- **Port admin** – Shows if the interface is enabled or disabled (i.e., up or down).
- **Speed-duplex** – Shows the current speed and duplex mode. (Auto, or fixed choice)
- **Capabilities** – Specifies the capabilities to be advertised for a port during auto-negotiation. (To access this item on the web, see "Configuring Interface Connections" on page 3-48.) The following capabilities are supported.
  - **10half** - Supports 10 Mbps half-duplex operation
  - **10full** - Supports 10 Mbps full-duplex operation
  - **100half** - Supports 100 Mbps half-duplex operation
  - **100full** - Supports 100 Mbps full-duplex operation
  - **1000full** - Supports 1000 Mbps full-duplex operation
  - **Sym** - Transmits and receives pause frames for flow control
  - **FC** - Supports flow control
- **Broadcast storm** – Shows if broadcast storm control is enabled or disabled.
- **Broadcast storm limit** – Shows the broadcast storm threshold. (500 - 262143 packets per second)
- **Flow control** – Shows if flow control is enabled or disabled.
- **LACP** – Shows if LACP is enabled or disabled.
- **Port Security** – Shows if port security is enabled or disabled.
- **Max MAC count** – Shows the maximum number of MAC address that can be learned by a port. (0 - 20 addresses)
- **Port security action** – Shows the response to take when a security violation is detected. (none, shutdown, trap, trap-and-shutdown)
- **Combo forced mode** – Shows the forced/preferred port type to use for combination ports 21-24. (copper forced, copper preferred auto, SFP forced, SFP preferred auto)

Current status:

- **Link Status** – Indicates if the link is up or down.
- **Operation speed-duplex** – Shows the current speed and duplex mode.
- **Port Operaton Status** – Indicates if the link is Up or Down.
- **Flow control type** – Indicates the type of flow control currently in use.

  (IEEE 802.3x, Back-Pressure or none)

CLI – This example shows the connection status for Port 5.

```
Console#show interfaces status ethernet 1/5                              4-93
Information of Eth 1/5
 Basic information:
  Port type: 1000T
  Mac address: 00-30-f1-47-58-46
 Configuration:
  Name:
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full, 1000full,
  Broadcast storm: Enabled
  Broadcast storm limit: 500 packets/second
  Flow control: Disabled
  Lacp: Disabled
  Port security: Disabled
  Max MAC count: 0
  Port security action: None
  Combo forced mode: None
 Current status:
  Link status: Down
  Port operation status: Up
  Operation speed-duplex: 100full
  Flow control type: None
Console#
```

Configuring Interface Connections

You can use the Port Configuration or Trunk Configuration page to enable/disable an interface, set auto-negotiation and the interface capabilities to advertise, or manually fix the speed, duplex mode, and flow control.

Command Attributes

- **Name** – Allows you to label an interface. (Range: 1-64 characters)
- **Admin** – Allows you to manually disable an interface. You can disable an interface due to abnormal behavior (e.g., excessive collisions), and then reenable it after the problem has been resolved. You may also disable an interface for security reasons.
- **Speed/Duplex** – Allows you to manually set the port speed and duplex mode.
- **Flow Control** – Allows automatic or manual selection of flow control.

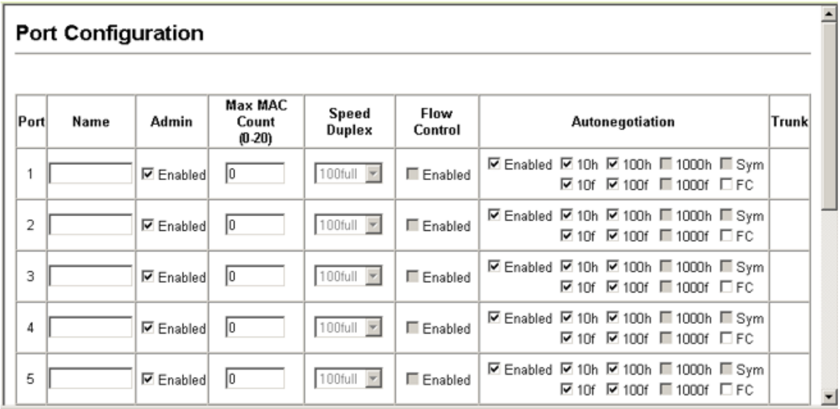
- **Autonegotiation (Port Capabilities)** – Allows auto-negotiation to be enabled/ disabled. When auto-negotiation is enabled, you need to specify the capabilities to be advertised. When auto-negotiation is disabled, you can force the settings for speed, mode, and flow control.The following capabilities are supported.
  - **10half** - Supports 10 Mbps half-duplex operation
  - **10full** - Supports 10 Mbps full-duplex operation
  - **100half** - Supports 100 Mbps half-duplex operation
  - **100full** - Supports 100 Mbps full-duplex operation
  - **1000full** - Supports 1000 Mbps full-duplex operation
  - **Sym** (Gigabit only) - Check this item to transmit and receive pause frames, or clear it to auto-negotiate the sender and receiver for asymmetric pause frames. (*The current switch chip only supports symmetric pause frames.*)
  - **FC** - Supports flow control

    Flow control can eliminate frame loss by “blocking” traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3x for full-duplex operation. (Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.)

    (Default: Autonegotiation enabled; Advertised capabilities for 1000BASE-T – 10half, 10full, 100half, 100full, 1000full; 1000BASE-SX/LX/LH – 1000full; 100BASE-TX – 100full)
- **Trunk** – Indicates if a port is a member of a trunk. To create trunks and select port members, see “Creating Trunk Groups” on page 3-44.

Note: Auto-negotiation must be disabled before you can configure or force the interface to use the Speed/Duplex Mode or Flow Control options.

Web – Click Port, Port Configuration or Trunk Configuration. Modify the required interface settings, and click Apply.



Port Configuration

Port	Name	Admin	Max MAC Count (0-20)	Speed Duplex	Flow Control	Autonegotiation	Trunk
1		☑ Enabled	0	100full	☐ Enabled	☑ Enabled ☑ 10h ☑ 100h ☐ 1000h ☐ Sym ☑ 10f ☑ 100f ☐ 1000f ☐ FC	
2		☑ Enabled	0	100full	☐ Enabled	☑ Enabled ☑ 10h ☑ 100h ☐ 1000h ☐ Sym ☑ 10f ☑ 100f ☐ 1000f ☐ FC	
3		☑ Enabled	0	100full	☐ Enabled	☑ Enabled ☑ 10h ☑ 100h ☐ 1000h ☐ Sym ☑ 10f ☑ 100f ☐ 1000f ☐ FC	
4		☑ Enabled	0	100full	☐ Enabled	☑ Enabled ☑ 10h ☑ 100h ☐ 1000h ☐ Sym ☑ 10f ☑ 100f ☐ 1000f ☐ FC	
5		☑ Enabled	0	100full	☐ Enabled	☑ Enabled ☑ 10h ☑ 100h ☐ 1000h ☐ Sym ☑ 10f ☑ 100f ☐ 1000f ☐ FC	

CLI – Select the interface, and then enter the required settings.

```
Console(config)#interface ethernet 1/12                              4-86
Console(config-if)#description RD SW#12                              4-87
Console(config-if)#shutdown                                          4-91
.
Console(config-if)#no shutdown
Console(config-if)#no negotiation                                    4-88
Console(config-if)#speed-duplex 100half                              4-87
Console(config-if)#flowcontrol                                       4-90
.
Console(config-if)#negotiation
Console(config-if)#capabilities 100half                              4-89
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
Console(config-if)#exit
```

Creating Trunk Groups

You can create multiple links between devices that work as one virtual, aggregate link. A port trunk offers a dramatic increase in bandwidth for network segments where bottlenecks exist, as well as providing a fault-tolerant link between two devices. You can create one trunk with two Gigabit optional module ports.

The switch supports both static trunking and dynamic Link Aggregation Control Protocol (LACP). Static trunks have to be manually configured at both ends of the link, and the switches must comply with the Cisco EtherChannel standard. On the other hand, LACP configured ports can automatically negotiate a trunked link with LACP-configured ports on another device. You can configure two Gigabit optional module ports as LACP, as long as they are not already configured as part of a static trunk. If ports on another device are also configured as LACP, the switch and the other device will negotiate a trunk link between them.

Command Usage

Besides balancing the load across each port in the trunk, the other ports provide redundancy by taking over the load if a port in the trunk fails. However, before making any physical connections between devices, use the web interface or CLI to specify the trunk on the devices at both ends. When using a port trunk, take note of the following points:

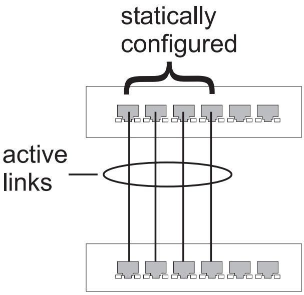
- Finish configuring port trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- You can create one trunk with two Gigabit optional module ports.
- The ports at both ends of a connection must be configured as trunk ports.
- When configuring static trunks on switches of different types, they must be compatible with the Cisco EtherChannel standard.
- The ports at both ends of a trunk must be configured in an identical manner, including communication mode (i.e., speed, duplex mode and flow control), VLAN assignments, and CoS settings.

- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- STP, VLAN, and IGMP settings can only be made for the entire trunk.

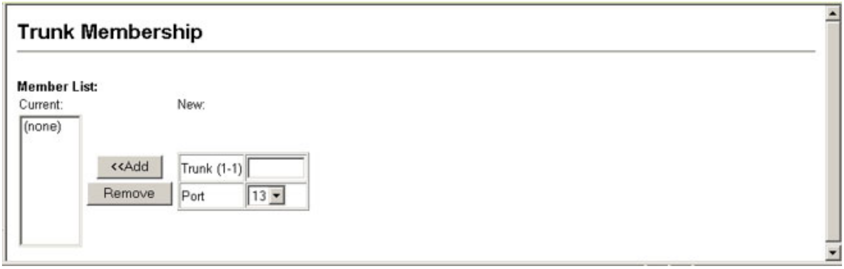
Statically Configuring a Trunk

Command Usage

- When configuring static trunks, you may not be able to link switches of different types, depending on the manufacturer's implementation. However, note that the static trunks on this switch are Cisco EtherChannel compatible.
- To avoid creating a loop in the network, be sure you add a static trunk via the configuration interface before connecting the ports, and also disconnect the ports before removing a static trunk via the configuration interface.



Web – Click Port, Trunk Membership. Enter a trunk ID of 1-6 in the Trunk field, select any of the switch ports from the scroll-down port list, and click Add. After you have completed adding ports to the member list, click Apply.



Trunk Membership

Member List:

Current: (none)

New:

Trunk (1-1)

Port 13

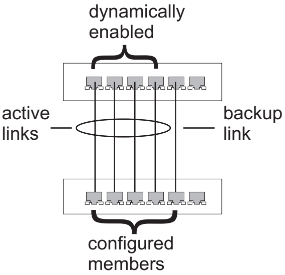
CLI – This example creates trunk 2 with ports 13 and 14. Just connect these ports to two static trunk ports on another switch to form a trunk.

```
Console(config)#interface port-channel 1                            4-86
Console(config-if)#exit
Console(config)#interface ethernet 1/13                             4-86
Console(config-if)#channel-group 1                                  4-101
Console(config-if)#exit
Console(config)#interface ethernet 1/14
Console(config-if)#channel-group 1
Console(config-if)#end
Console#show interfaces status port-channel 1                       4-93
Information of Trunk 1
 Basic information:
  Port type: 1000GBIC
  Mac address: 00-01-00-02-00-10
 Configuration:
  Name:
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 1000full,
  Flow control: Disabled
  Port security: Disabled
  Max MAC count: 0
 Current status:
  Created by: User
  Link status: Down
  Operation speed-duplex: 1000full
  Flow control type: None
  Member Ports: Eth1/13, Eth1/14,
Console#
```

Enabling LACP on Selected Ports

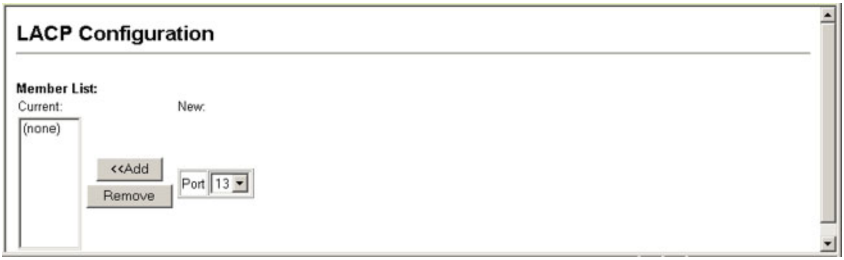
Command Usage

- To avoid creating a loop in the network, be sure you enable LACP before connecting the ports, and also disconnect the ports before disabling LACP.
- If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.
- A trunk formed with another switch using LACP will automatically be assigned the next available trunk ID.



- If more than four ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.
- All ports on both ends of an LACP trunk must be configured for full duplex, either by forced mode or auto-negotiation.

Web – Click Port, LACP, Configuration. Select switch ports from the scroll-down port list and click Add. After you have completed adding ports to the member list, click Apply.



LACP Configuration

Member List:

Current:

(none)

New:

Port 13

CLI – The following example enables LACP for ports 13 and 14. Just connect these ports to LACP-enabled trunk ports on another switch to form a trunk.

```
Console(config)#interface ethernet 1/13                                4-86
Console(config-if)#lacp                                                4-101
Console(config-if)#exit
Console(config)#interface ethernet 1/14
Console(config-if)#lacp
Console(config-if)#end
Console#show interfaces status port-channel 1                          4-93
Information of Trunk 1
 Basic information:
  Port type: 1000GBIC
  Mac address: 22-22-22-22-22-2d
 Configuration:
  Name:
  Port admin status: Up
  Speed-duplex: Auto
  Capabilities: 1000full,
  Flow control status: Disabled
  Port security: Disabled
  Max MAC count: 0
  Port security action: None
  Combo forced mode: None
 Current status:
  Created by: Lacp
  Link status: Up
  Port operation status: Up
  Operation speed-duplex: 1000full
  Flow control type: None
  Member Ports: Eth1/3, Eth1/14,
Console#
```

Setting Broadcast Storm Thresholds

Broadcast storms may occur when a device on your network is malfunctioning, or if application programs are not well designed or properly configured. If there is too much broadcast traffic on your network, performance can be severely degraded or everything can come to complete halt.

You can protect your network from broadcast storms by setting a threshold for broadcast traffic for each port. Any broadcast packets exceeding the specified threshold will then be dropped.

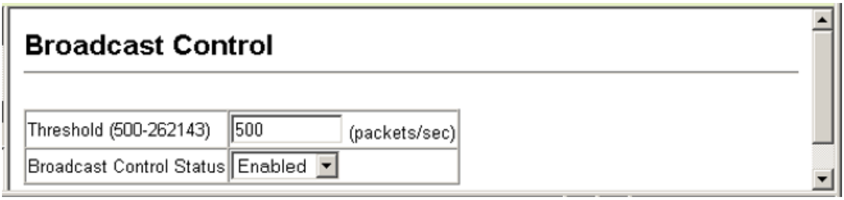
Command Usage

- Broadcast Storm Control is enabled by default.
- The default threshold is 500 packets per second.
- Broadcast control does not effect IP multicast traffic.
- The specified threshold applies to all ports on the switch.

Command Attributes

- Threshold – Threshold in packets per second. (Options: 500-262143 packets per second; Default: 500 packets per second)
- Broadcast Control Status – Shows whether or not broadcast storm control has been enabled. (Default: Enabled)

Web – Click Port, Broadcast Control. Set the threshold, set Broadcast Control Status to enabled, then click Apply.



Broadcast Control

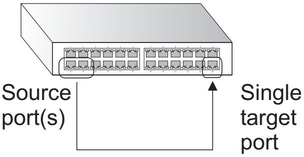
Threshold (500-262143)	500 (packets/sec)
Broadcast Control Status	Enabled

CLI – Specify any interface, and then enter the threshold. The following disables broadcast storm control for port 1, and then sets broadcast suppression at 600 packets per second for port 2. This threshold will then apply to all ports with broadcast storm control enabled.

```
Console(config)#interface ethernet 1/1                               4-86
Console(config-if)#no switchport broadcast                           4-91
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#switchport broadcast packet-rate 600              4-91
Console(config-if)#end
Console#show interfaces switchport ethernet 1/2
Information of Eth 1/2
 Broadcast threshold: Enabled, 600 packets/second
 Lacp status: Disabled
 Ingress rate limit: disable,100M bits per second
 Egress rate limit: disable,100M bits per second
 VLAN membership mode: Hybrid
 Ingress rule: Disabled
 Acceptable frame type: All frames
 Native VLAN: 1
 Priority for untagged traffic: 0 Allowed Vlan:    1(u),
 Forbidden Vlan:
Console#
```

Configuring Port Mirroring

You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.



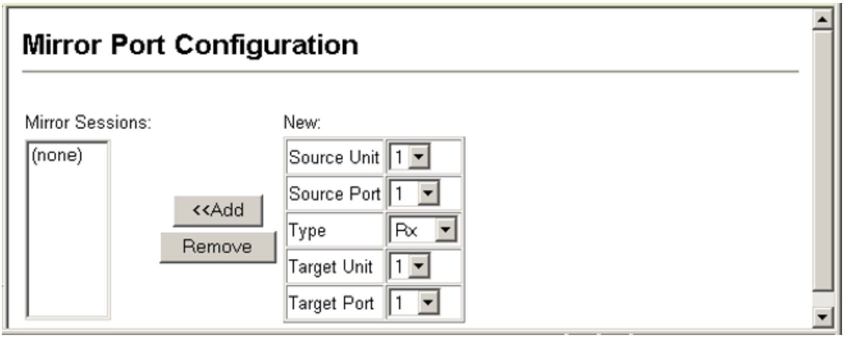
Command Usage

- Monitor port speed should match or exceed source port speed, otherwise traffic may be dropped from the monitor port.
- All mirror sessions have to share the same destination port.
- When mirroring port traffic, the target port must be included in the same VLAN as the source port.

Command Attributes

- **Mirror Sessions** – Displays a list of current mirror sessions.
- **Source Unit** – The switch containing the mirror source port. This switch does not support stacking , so this number will always be 1.
- **Source Port** – The port whose traffic will be monitored.
- **Type** – Allows you to select which traffic to mirror to the target port, Rx (receive), Tx (transmit), or Both.
- **Target Unit** – The switch containing the mirror target port. This switch does not support stacking , so this number will always be 1.
- **Target Port** – The port that will “duplicate” or “mirror” the traffic on the source port.

Web – Click Port, Mirror. Specify the source port, the traffic type to be mirrored, and the target port, then click Add.



Mirror Port Configuration

Mirror Sessions:

(none)

New:

Source Unit	1
Source Port	1
Type	Rx
Target Unit	1
Target Port	1

CLI – Use the interface command to select the monitor port, then use the port monitor command to specify the source port. Note that default mirroring under the CLI is for both received and transmitted packets.

```
Console(config)#interface ethernet 1/10                                  4-86
Console(config-if)#port monitor ethernet 1/13                            4-97
Console(config-if)#
```

Configuring Rate Limits

This function allows the network manager to control the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic coming out of the switch. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports or trunks. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped, conforming traffic is forwarded without any changes.

Command Attribute

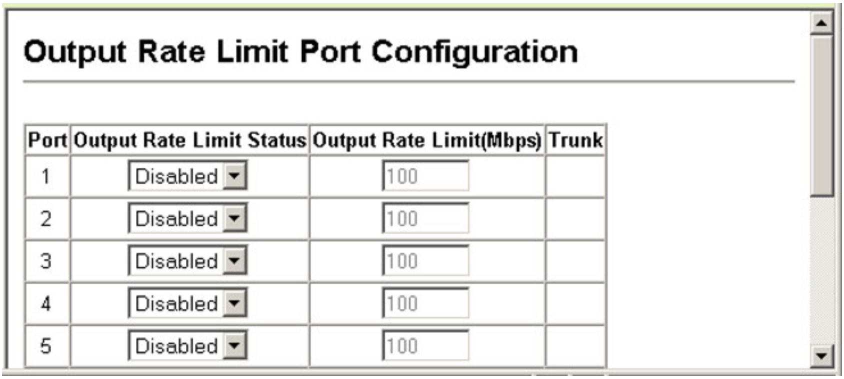
Rate Limit – Sets the output rate limit for an interface.

Default Status – Disabled

Default Rate – 100 Mbps for ports 1-12, 1000 Mbps for ports 13-14 with Gigabit modules installed.

Range – 1 - 1000 Mbps

Web - Click Rate Limit, Input/Output Port/Trunk Configuration. Set the Input Rate Limit Status or Output Rate Limit Status, then set the rate limit for the individual interfaces, and click Apply.



Output Rate Limit Port Configuration

Port	Output Rate Limit Status	Output Rate Limit(Mbps)	Trunk
1	Disabled	100	
2	Disabled	100	
3	Disabled	100	
4	Disabled	100	
5	Disabled	100	

CLI - This example sets the rate limit for input and output traffic passing through port 1 to 50 Mbps.

```
Console(config)#interface ethernet 1/1                                  4-86
Console(config-if)#rate-limit input 50                                  4-99
Console(config-if)#rate-limit output 50                                 4-99
Console(config-if)#
```

Showing Port Statistics

You can display standard statistics on network traffic from the Interfaces Group and Ethernet-like MIBs, as well as a detailed breakdown of traffic based on the RMON MIB. Interfaces and Ethernet-like statistics display errors on the traffic passing through each port. This information can be used to identify potential problems with the switch (such as a faulty port or unusually heavy loading). RMON statistics provide access to a broad range of statistics, including a total count of different frame types and sizes passing through each port. All values displayed have been accumulated since the last system reboot, and are shown as counts per second. Statistics are refreshed every 60 seconds by default.

Note: RMON groups 2, 3 and 9 can only be accessed using SNMP management software such as AccView.

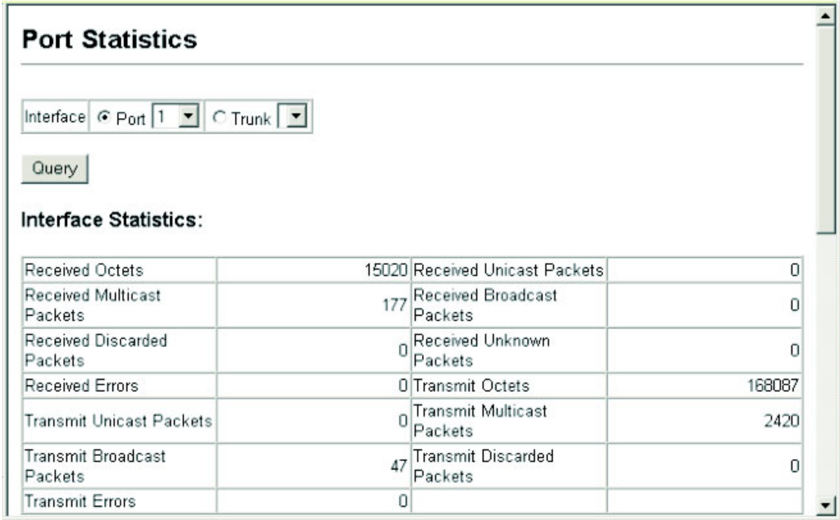
Statistical Values

Parameter	Description
Interface Statistics	
Received Octets	The total number of octets received on the interface, including framing characters.
Received Unicast Packets	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Received Multicast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer.
Received Broadcast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer.
Received Discarded Packets	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Received Unknown Packets	The number of packets received via the interface which were discarded because of an unknown or unsupported protocol.
Received Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Transmit Octets	The total number of octets transmitted out of the interface, including framing characters.
Transmit Unicast Packets	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Transmit Multicast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent.
Transmit Broadcast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.
Transmit Discarded Packets	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Transmit Errors	The number of outbound packets that could not be transmitted because of errors.
Etherlike Statistics	
Alignment Errors	The number of alignment errors (missynchronized data packets).
Late Collisions	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
FCS Errors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error.
Excessive Collisions	A count of frames for which transmission on a particular interface fails due to excessive collisions. This counter does not increment when the interface is operating in full-duplex mode.

Parameter	Description
Single Collision Frames	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Internal MAC Transmit Errors	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error.
Multiple Collision Frames	A count of successfully transmitted frames for which transmission is inhibited by more than one collision.
Carrier Sense Errors	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
SQE Test Errors	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface.
Frames Too Long	A count of frames received on a particular interface that exceed the maximum permitted frame size.
Deferred Transmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
Internal MAC Receive Errors	A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error.
RMON Statistics	
Drop Events	The total number of events in which packets were dropped due to lack of resources.
Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error.
Received Bytes	Total number of bytes of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
Received Frames	The total number of frames (bad, broadcast and multicast) received.
Broadcast Frames	The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets.
Multicast Frames	The total number of good frames received that were directed to this multicast address.
CRC/Alignment Errors	The number of CRC/alignment errors (FCS or alignment errors).
Undersize Frames	The total number of frames received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Oversize Frames	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.

Parameter	Description
64 Bytes Frames	The total number of frames (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
65-127 Byte Frames 128-255 Byte Frames 256-511 Byte Frames 512-1023 Byte Frames 1024-1518 Byte Frames 1519-1536 Byte Frames	The total number of frames (including bad packets) received and transmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets).

Web – Click Port, Port Statistics. Select the required interface, and click Query. You can also use the Refresh button at the bottom of the page to update the screen.

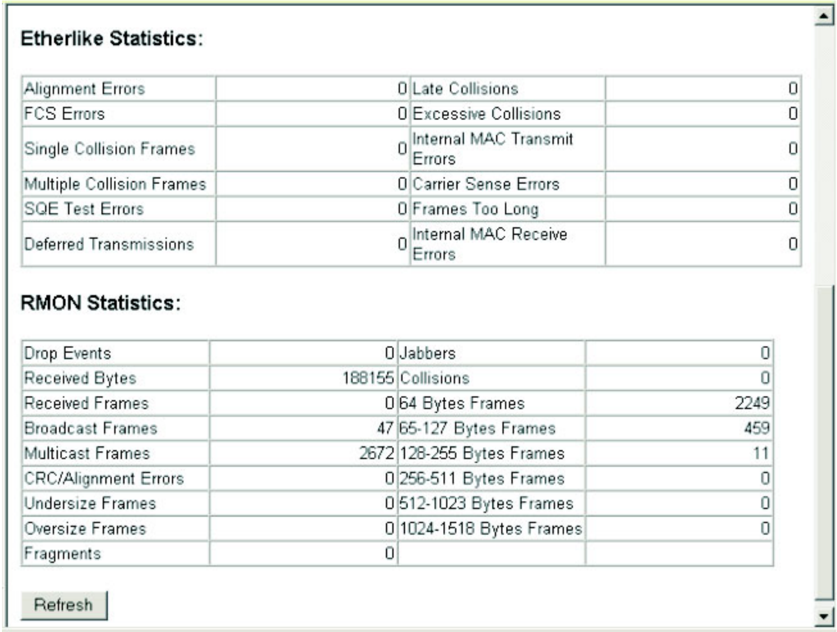


Port Statistics

Interface ● Port 1 ○ Trunk

Interface Statistics:

Received Octets	15020	Received Unicast Packets	0
Received Multicast Packets	177	Received Broadcast Packets	0
Received Discarded Packets	0	Received Unknown Packets	0
Received Errors	0	Transmit Octets	168087
Transmit Unicast Packets	0	Transmit Multicast Packets	2420
Transmit Broadcast Packets	47	Transmit Discarded Packets	0
Transmit Errors	0		



Etherlike Statistics:

Alignment Errors	0	Late Collisions	0
FCS Errors	0	Excessive Collisions	0
Single Collision Frames	0	Internal MAC Transmit Errors	0
Multiple Collision Frames	0	Carrier Sense Errors	0
SQE Test Errors	0	Frames Too Long	0
Deferred Transmissions	0	Internal MAC Receive Errors	0

RMON Statistics:

Drop Events	0	Jabbers	0
Received Bytes	188155	Collisions	0
Received Frames	0	64 Bytes Frames	2249
Broadcast Frames	47	65-127 Bytes Frames	459
Multicast Frames	2672	128-255 Bytes Frames	11
CRC/Alignment Errors	0	256-511 Bytes Frames	0
Undersize Frames	0	512-1023 Bytes Frames	0
Oversize Frames	0	1024-1518 Bytes Frames	0
Fragments	0		

CLI – This example shows statistics for port 12.

```
Console#show interfaces counters ethernet 1/12                      4-94
Ethernet 1/12
 Iftable stats:
  Octets input: 868453, Octets output: 3492122
  Unicast input: 7315, Unitcast output: 6658
  Discard input: 0, Discard output: 0
  Error input: 0, Error output: 0
  Unknown protos input: 0, QLen output: 0
 Extended iftable stats:
  Multi-cast input: 0, Multi-cast output: 17027
  Broadcast input: 231, Broadcast output: 7
 Ether-like stats:
  Alignment errors: 0, FCS errors: 0
  Single Collision frames: 0, Multiple collision frames: 0
  SQE Test errors: 0, Deferred transmissions: 0
  Late collisions: 0, Excessive collisions: 0
  Internal mac transmit errors: 0, Internal mac receive errors: 0
  Frame too longs: 0, Carrier sense errors: 0
  Symbol errors: 0
 RMON stats:
  Drop events: 0, Octets: 4422579, Packets: 31552
  Broadcast pkts: 238, Multi-cast pkts: 17033
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
  CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets: 25568, Packet size 65 to 127 octets: 1616
  Packet size 128 to 255 octets: 1249, Packet size 256 to 511 octets: 1449
  Packet size 512 to 1023 octets: 802, Packet size 1024 to 1518 octets: 871
```

VDSL Configuration

You can configure and display communication parameters for VDSL and Ethernet ports on the switch and connected CPEs.

VDSL Global Configuration

Assigns the same profile to each VDSL switch port. Details of these profiles are given in the table below.

Profile Name	ProfileType	Downstream Rate (Mbps)	Upstream Rate (Mbps)
Default	Public	1.20	1.40
A1-02OAG-R1	Public	7.56	2.43
A2-02OAG-R1	Public	10.80	2.43
A3-01OAG-R1	Public	17.28	3.78
A4-01OAG-R1	Public	25.92	4.72
S1-03OAG-R1	Public	7.56	7.56
S2-03OAG-R1	Public	10.80	10.40
S3-00OAG-R1	Public	17.28	16.47
S1-16-16	Private	16.74	16.20
S2-16-16A	Private	16.74	16.20
A1-34-11	Private	33.75	11.34
A2-34-11A	Private	33.75	11.34
A3-25-3	Private	25.38	3.24
A4-45-5	Private	44.55	5.13
A5-50-7	Private	50.49	7.29
A6-22-3A	Private	22.55	3.24
A7-40-5A	Private	40.91	5.13
A8-46-7A	Private	46.44	7.29
TLAN	Private	17.01	5.40
Max-Rate	Private	71.28	40.50

Notes:

1. The VDSL Intelligent Switch uses Ethernet in the First Mile (EFM), a VDSL-based technology.
2. A suffix of “A” in the profile name (e.g., S2-16-16A) indicate that this profile is for both VDSL and ADSL lines in a bundle. Profiles without a suffix of “A” in the profile name (e.g., S1-16-16) are for VDSL lines only.
3. The following profiles are recommended for use with this switch; S1-16-16, S2-16-16A, A1-34-11, and A2-34-11A.

4. The maximum distances for VDSL links using the recommended profiles are:

Upstream	Downstream	Mode	Max. Range
16 Mbps	16 Mbps	Symetric	600m (1970 ft)
11 Mbps	34 Mbps	Asymetric	610m (2000 ft)

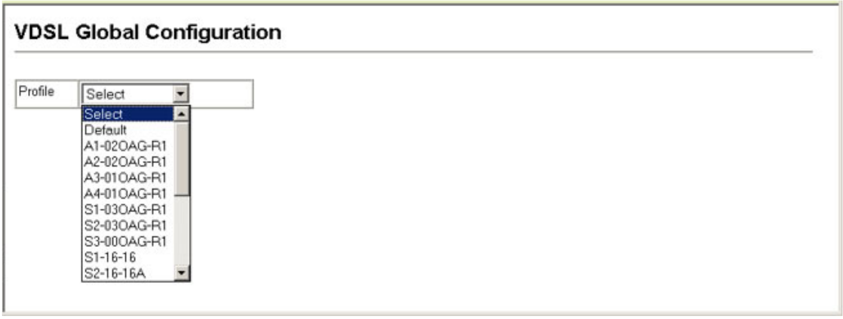
5. Type-1 26 AWG (100 ohm)/0.4 mm, or Type-2 24 AWG (100 ohm)/0.5 mm cable may be installed to achieve the maximum distance, however, typically, 24 AWG (100 ohm)/0.5 mm wire is better than 26 AWG (100 ohm)/0.4 mm wire. Note that the distance may be limited by factors such as how the cable is bundled, and the interference and noise on the link.

6. Public profiles conform to specific standards such as ANSI or ETSI. Private profiles do not conform to these standards.

Command Attributes

- **Profile Name** – The name for the specific set of communication parameters.
- **Profile Type** – Public profiles are those that meet specific standards e.g., ETSI or ANSI. Private profiles do not meet these standards. The ports on a VDSL switch can be assigned the same or different profiles.
- **Downstream Rate** – Rate of data transmission from the switch to the CPE.
- **Upstream Rate** – Rate of data transmission from the CPE to the switch.

Web – Click VDSL, Global Configuration, and select a profile from the drop-down list.



VDSL Global Configuration

Profile: Select

CLI – This example shows configuring the switch to profile S1-16-16.

Example

```
Console#config
Console(config)#efm profile global S1-16-16                     4-103
Console(config)#
```

VDSL Port Configuration

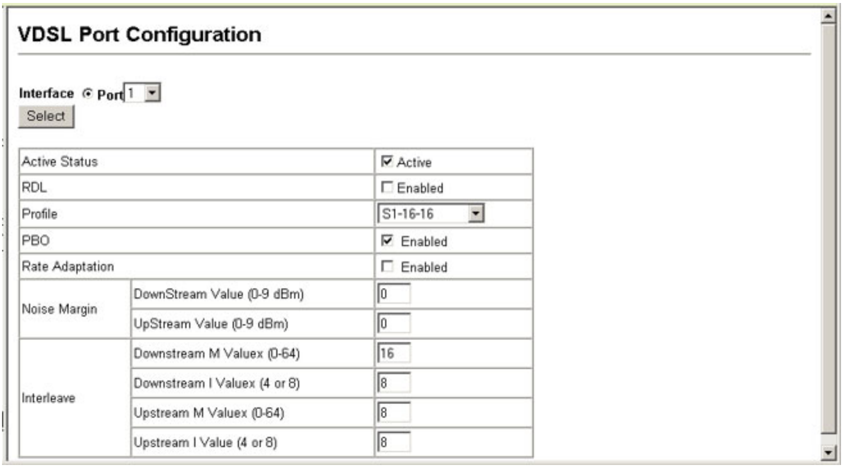
You can enable/disable a selected port, enable disable Remote Digital Loopback (RDL), set the optimal transmission rate, and configure a profile for the selected port.

Command Attributes

- **Active Status** – Check this box to enable the selected port.
- **RDL** – Check this box to enable Remote Digital Loopback (RDL). Remote Digital Loopback (RDL) tests the link between the switch and the CPE by sending out, and returning data through the CPE, over the VDSL link (see “efm rdl” on page 4-107). (Default: Disabled)
- **Profile** – Configures a profile for the selected port.
- **PBO** – Enables/disables power back-off on the selected port. If PBO is enabled the power of transmission from the port will automatically be adjusted to ensure that the signal successfully reaches the reception port.
- **Rate Adaptation** – The data rate on a VDSL line can be affected by factors such as temperature, humidity, and electro-magnetic radiation. When rate adaption is enabled, the switch will determine the optimal transmission rate for the current conditions.
- **Noise Margin** – The noise margin indicates how much the noise on the selected VDSL can increase before the signal is affected. As the noise on the line increases, the margin will approach zero. If the noise exceeds the current noise margin, the signal will be lost. You will then need to increase the margin until the signal is restored.
  Range; 0-9 dBm. Default: 0 dBm
- **Interleave** – Interleaving on the improves Reed Solomon error correction when there is pulse noise. A greater degree of interleaving will provide more protection against pulse noise but will increase transmission delay and reduce the effective bandwidth of the link. The degree of interleaving can be increased by increasing M or I.
  - **M** – The interleaving depth index.
    Range: 0-64, Upstream default value: 8, Downstream default value:16
  - **I** – The interleaver block length.
    Range: 4 or 8; Upstream default value: 8, Downstream default value: 8

Web Interface

Click VDSL, Port Configuration,select a port from the drop-down list, and click Select..



VDSL Port Configuration

Interface ● Port 1

Select

Active Status		☑ Active
RDL		□ Enabled
Profile		S1-16-16
PBO		☑ Enabled
Rate Adaptation		□ Enabled
Noise Margin	DownStream Value (0-9 dBm)	0
	UpStream Value (0-9 dBm)	0
Interleave	Downstream M Valuex (0-64)	16
	Downstream I Valuex (4 or 8)	8
	Upstream M Valuex (0-64)	8
	Upstream I Value (4 or 8)	8

Command Line Interface

The following examples show how these features are configured in the CLI.

Example

The following example disables VDSL port 1.

```
Console (config)#interface ethernet 1/1                           4-86
Console(config-if)#efm shutdown                                   4-106
Console(config-if)#
```

Example

The following example shows how to enable/disable RDL on VDSL port 1.

```
Console (config)#interface ethernet 1/1                           4-86
Console(config-if)#efm rdl                                        4-107
Console(config-if)#no efm rdl
Console(config-if)#
```

Example

The following example shows efm profile S1-16-16 assigned to VDSL port 1.

```
Console#config
Console(config)#interface ethernet 1/1                            4-86
Console(config-if)#efm profile S1-16-16                           4-105
Console(config-if)#
```

VDSL Port Link Status

Command Attributes

- **General Status**
  - **Link** – Shows the status of the VDSL link.
  - **Noise Margin** – The noise margin indicates how much the noise on the selected VDSL port can increase before the signal is affected. As the noise on the line increases, the margin will approach zero. If the noise exceeds the current noise margin, the signal will be lost. You will then need to increase the margin until the signal is restored.

    Range: 0-9 dBm. Default: 0 dBm
- **PMD* Status**
  - **SNR (dB)** –The signal-to-noise ratio of the VDSL line.
  - **Downstream Rate (Mbps)** – The rate at which data is transmitted from the switch to the CPE.
  - **Upstream Rate (Mbps)** – The rate at which data is transmitted from the CPE to the switch.
  - **PBO** – Indicates the status of the power back-off mechanism (on/off). If PBO is enabled the power of transmission from the port will automatically be adjusted to ensure that the signal successfully reaches the reception port.
  - **Rate Adaptation** – The data rate on a VDSL line can be affected by factors such as temperature, humidity, and electro-magnetic radiation. When rate adaption is enabled, the switch will determine the optimal transmission rate for the current conditions.

* Physical Media Dependent

- **PMS-TC* Status**
  - **Reed-Solomon Errors** – The number of errors in data that have been corrected by the Reed-Solomon code.
  - **Interleave** – Interleaving improves Reed Solomon error correction when there is pulse noise. A greater degree of interleaving will provide more protection against pulse noise but will increase transmission delay and reduce the effective bandwidth of the link. The degree of interleaving can be increased by increasing M or I.
    - **M** – The interleaving depth index.

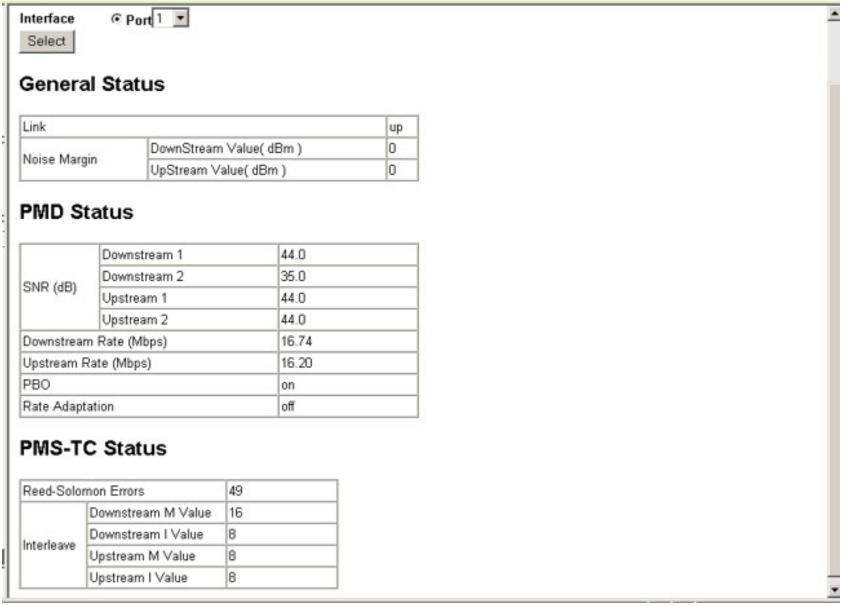
      Range: 0-64, Upstream default value: 8, Downstream default value: 16
    - **I** – The interleaving block length.

      Range: 4 or 8; Upstream default value: 8, Downstream default value: 8 protection.

* Physical Medium Specific Transmission Convergence

Web Interface

Click VDSL, Port Link Status.



General Status

Link		up
Noise Margin	DownStream Value(dBm)	0
	UpStream Value(dBm)	0

PMD Status

SNR (dB)	Downstream 1	44.0
	Downstream 2	35.0
	Upstream 1	44.0
	Upstream 2	44.0
Downstream Rate (Mbps)		16.74
Upstream Rate (Mbps)		16.20
PBO		on
Rate Adaptation		off

PMS-TC Status

Reed-Solomon Errors		49
Interleave	Downstream M Value	16
	Downstream I Value	8
	Upstream M Value	8
	Upstream I Value	8

Command Line Interface

The following example displays VDSL link current values on VDSL switch port 2.

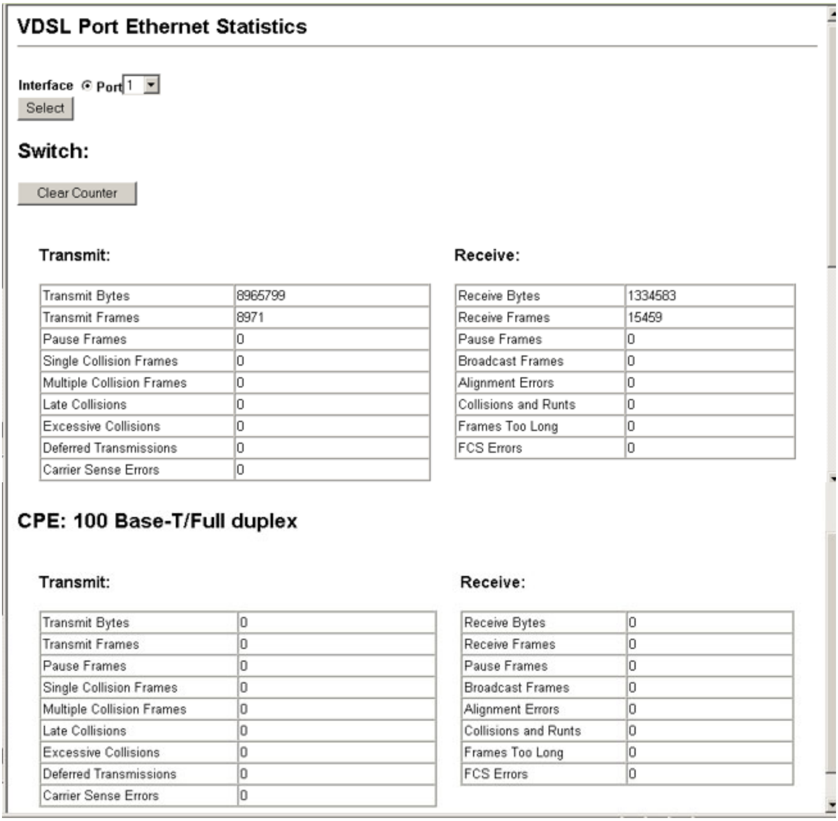
Example

```
Console#show controller efm Ethernet 1/2 actual dsrserrs              4-113
 Downstream Reed-Solomon errors: 0
Console#show controller efm Ethernet 1/2 actual link
 Link status: Down
Console#show controller efm Ethernet 1/2 actual rxpower
 Local receive power: 26.00 dBm/Hz
Console#show controller lre Ethernet 1/2 actual snr
 SNR: 27.00 dB
Console#show controller efm Ethernet 1/2 actual txpower
 Remote transmit power: -89.70 dBm/Hz
Console#show controller efm Ethernet 1/2 actual usrserrs
 Upstream Reed-Solomon errors: 0
Console#
```

Displaying VDSL Port Ethernet Statistics

VDSL Port Ethernet Statistics displays key statistics for an interface.

Web – Click VDSL, VDSL Port Ethernet Statistics.



VDSL Port Ethernet Statistics

Interface ● Port 1

Switch:

Transmit:

Transmit Bytes	8965799
Transmit Frames	8971
Pause Frames	0
Single Collision Frames	0
Multiple Collision Frames	0
Late Collisions	0
Excessive Collisions	0
Deferred Transmissions	0
Carrier Sense Errors	0

Receive:

Receive Bytes	1334583
Receive Frames	15459
Pause Frames	0
Broadcast Frames	0
Alignment Errors	0
Collisions and Runts	0
Frames Too Long	0
FCS Errors	0

CPE: 100 Base-T/Full duplex

Transmit:

Transmit Bytes	0
Transmit Frames	0
Pause Frames	0
Single Collision Frames	0
Multiple Collision Frames	0
Late Collisions	0
Excessive Collisions	0
Deferred Transmissions	0
Carrier Sense Errors	0

Receive:

Receive Bytes	0
Receive Frames	0
Pause Frames	0
Broadcast Frames	0
Alignment Errors	0
Collisions and Runts	0
Frames Too Long	0
FCS Errors	0

CLI – Use the **show interfaces counters** command.

Example

```
Console#show interfaces counters ethernet 1/11                         4-94
Ethernet 1/11
 Iftable stats:
  Octets input: 19648, Octets output: 714944
  Unitcast input: 0, Unitcast output: 0
  Discard input: 0, Discard output: 0
  Error input: 0, Error output: 0
  Unknown protos input: 0, QLen output: 0
 Extended iftable stats:
  Multi-cast input: 0, Multi-cast output: 10524
  Broadcast input: 136, Broadcast output: 0
Ether-like stats:
  Alignment errors: 0, FCS errors: 0
  Single Collision frames: 0, Multiple collision frames: 0
  SQE Test errors: 0, Deferred transmissions: 0
  Late collisions: 0, Excessive collisions: 0
  Internal mac transmit errors: 0, Internal mac receive errors: 0
  Frame too longs: 0, Carrier sense errors: 0
Symbol errors: 0
RMON stats:
  Drop events: 0, Octets: 734720, Packets: 10661
  Broadcast pkts: 136, Multi-cast pkts: 10525
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
  CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets: 9877, Packet size 65 to 127 octets: 93
  Packet size 128 to 255 octets: 691, Packet size 256 to 511 octets: 0
  Packet size 512 to 1023 octets: 0, Packet size 1024 to 1518 octets: 0
Console#
```

VDSL Line Configuration

Command Attributes

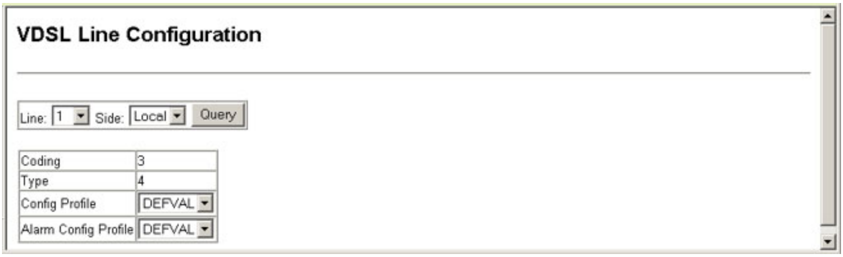
- **Line** – Select the VDSL line for configuration from the drop-down list.
- **Local/Remote** – In this version this may only be set to Local, indicating that the line configuration applies to the line connection from the switch to the CPE.
- **Coding** – Specifies the VDSL coding type used on this line.

  The types of code are:
  1. Others (none of the following)
  2. Multiple Carrier Modulation
  3. Single Carrier Modulation
- **Type** – Defines the type of VDSL physical line by defining whether and how the line is channelized.

  The types of line are:
  1. No channels exist
  2. Only fast channels exist
  3. Only interleaved channels exists
  4. Either fast or interleaved channels exist
  5. Both fast and interleaved channels exist
- **Config Profile** – In this version, only “DEFVAL” is displayed. In future versions, a drop-down list of all configurable VDSL profiles will be in this field.
- **Alarm Config Profile** – The alarm profile is pre-configured to send trap messages via SNMP protocol to register errors on the VDSL line.

Web Interface

Click VDSL, Line Configuration, select the line from the drop-down list, and click Query.



VDSL Line Configuration

Line: 1 Side: Local

Coding	3
Type	4
Config Profile	DEFVAL
Alarm Config Profile	DEFVAL

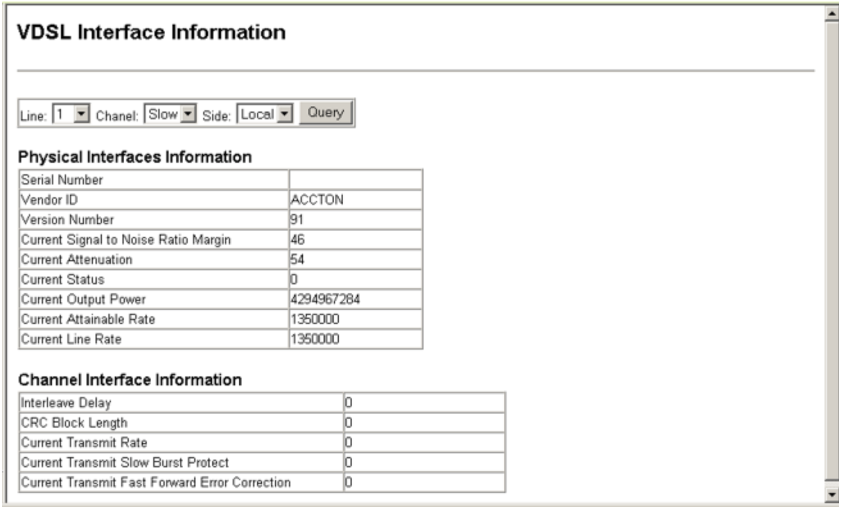
Displaying VDSL Interface Information

Command Attributes

- **Line** – Select the VDSL line from the drop-down list.
- **Channel** – Select Slow or Fast from the drop-down menu. The switch uses the slow channel for data that requires a very low error rate in transmission. The switch uses the fast channel for data such as voice/video signals that require fast delivery, but for which a small error rate is acceptable.
- **Side** – This only displays Local. All information displayed is for data transmission from the switch to the CPE.
- **Physical Interfaces Information**
  - **Serial Number** – A number given by the manufacturer to the item produced. This only displays on the CPE side.
  - **Vendor ID** – The name of the manufacturer of this switch.
  - **Version Number** – The number of the current hardware.
  - **Current Signal to Noise Ratio Margin** – The noise margin indicates how much the noise on the selected VDSL can increase before the signal is affected. As the noise on the line increases, the margin will approach zero. If the noise exceeds the current noise margin, the signal will be lost. You will then need to increase the margin until the signal is restored.
    Range: 0-9 dBm Default: 0 dBm
  - **Current Attenuation** – The attenuation of the signal.
    Units: db
  - **Current Status** – This displays defects in the VDSL line in the current version, this always displays 0, which means no defects.
  - **Current Output Power** – The total output power transmitted on this line.
    Units: 0.1 dBm.
  - **Current Attainable Rate** – The maximum line data rate using the current profile.
    Unit: bits per second
  - **Current Line Rate** – The current line data rate.
    Unit: bits per second
- **Channel Interface Information**
  - **Interleave Delay** – Transmission delay caused by the use of interleaving.
    Units: milliseconds
  - **CRC Block Length** – Cyclic Redundancy Code (CRC) is a number derived from, and transmitted with, data frames in order to detect corruption of data.
  - **Current Transmit Rate*** – The current rate of data transmission.
  - **Current Transmit Slow Burst Protect*** – Actual level of impulse noise (burst) protection for an interleaved (slow) channel. This parameter is not applicable to fast channels. For fast channels, a value of zero is returned.
  - **Current Transmit Fast Forward Error Correction*** – Actual Forward Error Correction (FEC) redundancy related overhead for a fast channel. This parameter is not applicable to an interleaved (slow) channel. For interleaved channels, a value of zero shall be returned.

* Not supported in the current version

Web – Click VDSL, Interface Information select Line, Channel, and Side from the drop-down lists, and click Query.



VDSL Interface Information

Line: 1 Chanel: Slow Side: Local

Physical Interfaces Information

Serial Number	
Vendor ID	ACCTON
Version Number	91
Current Signal to Noise Ratio Margin	46
Current Attenuation	54
Current Status	0
Current Output Power	4294967284
Current Attainable Rate	1350000
Current Line Rate	1350000

Channel Interface Information

Interleave Delay	0
CRC Block Length	0
Current Transmit Rate	0
Current Transmit Slow Burst Protect	0
Current Transmit Fast Forward Error Correction	0

VDSL Performance Monitor Information

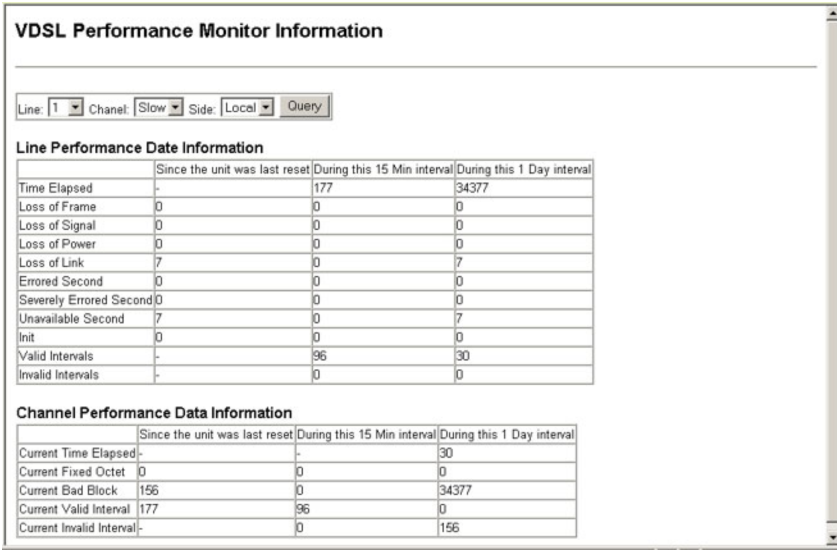
This screen displays line and channel performance data information since the switch was last reset, during the current 15 minute interval, and during the current day.

Command Attributes

- **Line** – Select the VDSL line from the drop-down list.
- **Chanel** – Select Slow or Fast from the drop-down menu. The switch uses the slow channel for data that requires a very low error rate in transmission. The switch uses the fast channel for data such as voice/video signals that require fast delivery, but for which a small error rate is acceptable
- **Side** – This only displays Local. All information displayed is for data transmission from the switch to the CPE.

- **Line Performance Date Information**
  - **Loss of Frame** (LOF) – Number of seconds that there was loss of framing, since the switch was last reset, or in the indicated time interval, .
  - **Loss of Signal** (LOS) – Number of seconds that there was loss of signal, since the switch was last reset, or in the indicated time interval.
  - **Loss of Power** – Number of seconds that there was loss of power, since the switch was last reset, or in the indicated time interval.
  - **Loss of Link** – Number of seconds that there was loss of link, since the switch was last reset, or in the indicated time interval.
  - **Errored Second** – Number of Errored Seconds since the switch was last reset, or in the indicated time interval. An Errored Second is a one-second interval containing one or more CRC anomalies, or one or more LOS or LOF defects.
  - **Severely Errored Second** – Number of Severely Errored Seconds since the switch was last reset, or in the indicated time interval. An Errored Second is a one-second interval containing one or more CRC anomalies, or one or more LOS or LOF defects.
  - **Unavailable Second** – Numberof Unavailable Seconds since the switch was last reset, or in the indicated time interval.
  - **Init** – Number of line initialization attempts since the switch was last reset, or in the indicated time interval. This count includes both successful and failed attempts.
  - **Valid intervals** – The number of intervals within which errors have been detected.
  - **Invalid Intervals** – The number of intervals within which no errors have been detected.

Web – Click VDSL, Performance Monitor Information.



VDSL Performance Monitor Information

Line Performance Date Information

	Since the unit was last reset	During this 15 Min interval	During this 1 Day interval
Time Elapsed	-	177	34377
Loss of Frame	0	0	0
Loss of Signal	0	0	0
Loss of Power	0	0	0
Loss of Link	7	0	7
Errored Second	0	0	0
Severely Errored Second	0	0	0
Unavailable Second	7	0	7
Init	0	0	0
Valid Intervals	-	96	30
Invalid Intervals	-	0	0

Channel Performance Data Information

	Since the unit was last reset	During this 15 Min interval	During this 1 Day interval
Current Time Elapsed	-	-	30
Current Fixed Octet	0	0	0
Current Bad Block	156	0	34377
Current Valid Interval	177	96	0
Current Invalid Interval	-	0	156

Monitoring VDSL Performance History

This screen displays line and channel performance data information during selected 15 minute intervals over the last 24 hours of switch operation, and during selected 1-day intervals from the current day to 30 days ago.

Command Attributes

- **Line** – Select the VDSL line from the drop-down list.
- **Chanel** – Select Slow or Fast from the drop-down list.
- **Side** – This only displays Local. All information displayed is for data transmission from the switch to the CPE.
- **Line Performance Date History Information**

  For the 15 Min Interval column, 1 is the most recent previous interval; interval 96 is 24 hours ago. Intervals 2 to 96 are optional.

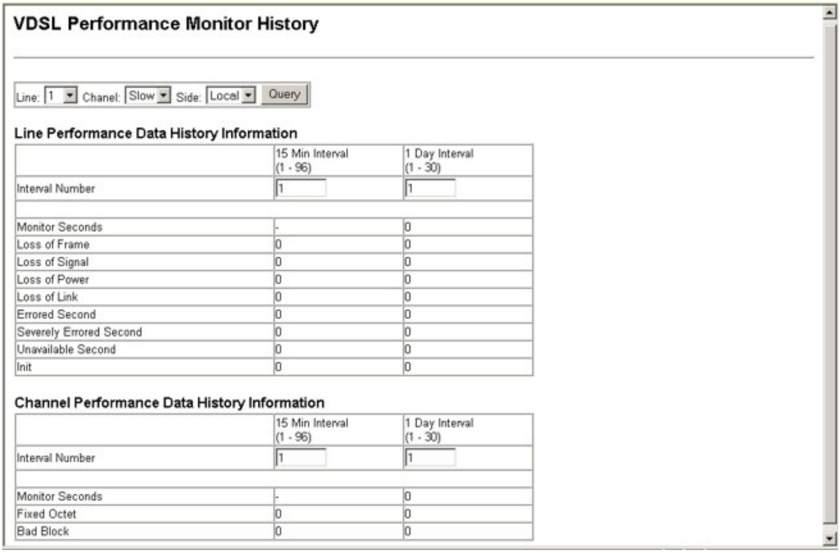
  For the 1 Day Interval column, Interval 1 is the most recent previous day; interval 30 is 30 days ago. Intervals 2 to 30 are optional.

  - **Loss of Frame** (LOF) – Number of seconds that there was loss of framing, in the indicated time interval.
  - **Loss of Signal** (LOS) – Number of seconds that there was loss of signal, in the indicated time interval.
  - **Loss of Power** – Number of seconds that there was loss of power, in the indicated time interval.

- **Loss of Link** – Number of seconds that there was loss of link, in the indicated time interval.
- **Errored Second** – Number of errored seconds in the indicated time interval. An errored second is a one-second interval containing one or more CRC anomalies, or one or more LOS or LOF defects.
- **Severely Errored Second** – Number of severely errored seconds in the indicated time interval. An errored second is a one-second interval containing one or more one or more CRC anomalies, or one or more LOS or LOF defects.
- **Unavailable Second** – Count of unavailable seconds in the indicated time interval.
- **Init** – Number of line initialization attempts in the indicated time interval. This count includes both successful and failed attempts.

- **Channel Performance Date History Information**
  - **Fixed Octet** – Number of corrected octets in the indicated time interval.
  - **Bad Block** – Number of uncorrectable blocks in the indicated time interval.

Web – Click VDSL, Performance Monitor History.



VDSL Performance Monitor History

Line: 1 Chanel: Slow Side: Local

Line Performance Data History Information

	15 Min Interval (1 - 96)	1 Day Interval (1 - 30)
Interval Number	1	1
Monitor Seconds	-	0
Loss of Frame	0	0
Loss of Signal	0	0
Loss of Power	0	0
Loss of Link	0	0
Errored Second	0	0
Severely Errored Second	0	0
Unavailable Second	0	0
Init	0	0

Channel Performance Data History Information

	15 Min Interval (1 - 96)	1 Day Interval (1 - 30)
Interval Number	1	1
Monitor Seconds	-	0
Fixed Octet	0	0
Bad Block	0	0

Address Table Settings

Switches store the addresses for all known devices. This information is used to pass traffic directly between the inbound and outbound ports. All the addresses learned by monitoring traffic are stored in the dynamic address table. You can also manually configure static addresses that are bound to a specific port.

Setting Static Addresses

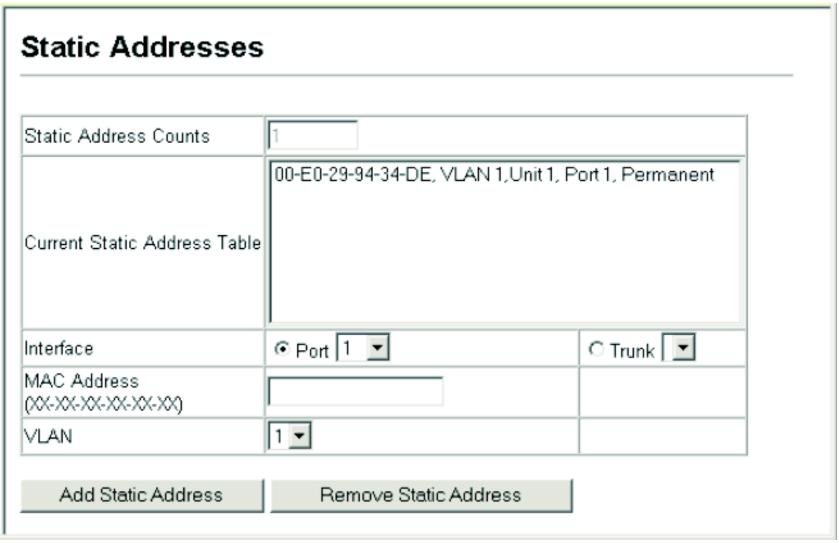
A static address can be assigned to a specific interface on this switch. Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.

Command Attributes

- **Static Address Counts*** – The number of manually configured addresses.
- **Current Static Address Table** – Lists all the static addresses.
- **Interface** – Port or trunk associated with the device assigned a static address.
- **MAC Address** – Physical address of a device mapped to this interface.
- **VLAN** – ID of configured VLAN (1-4094).

*Web Only

Web – Click Address Table, Static Addresses. Specify the interface, the MAC address and VLAN, then click Add Static Address.



Static Addresses

Static Address Counts	1	
Current Static Address Table	00-E0-29-94-34-DE, VLAN 1,Unit 1, Port 1, Permanent	
Interface	● Port 1	○ Trunk
MAC Address (XX-XX-XX-XX-XX-XX)		
VLAN	1	

CLI – This example adds an address to the static address table, but sets it to be deleted when the switch is reset.

```
Console(config)#mac-address-table static 00-e0-29-94-34-de interface
 ethernet 1/1 vlan 1 delete-on-reset                              4-120
Console(config)#
```

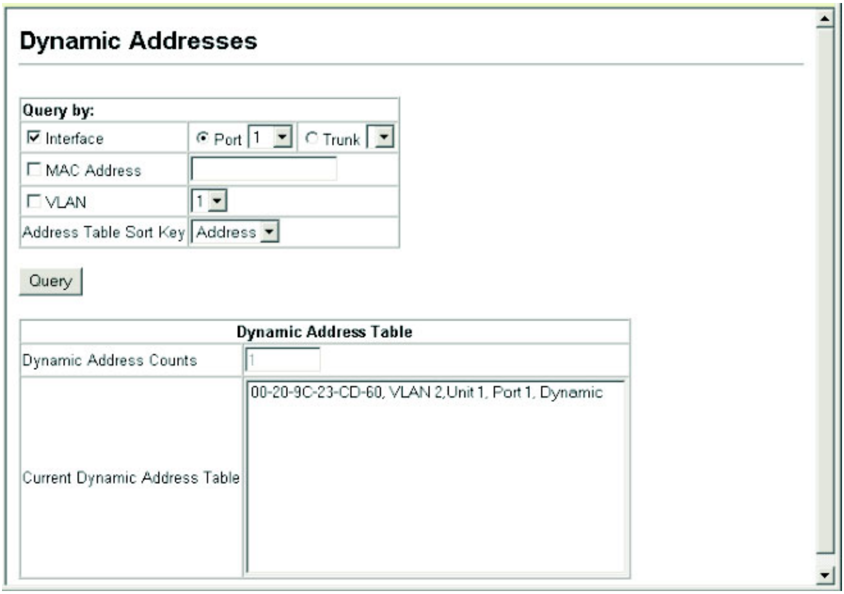
Displaying the Address Table

The Dynamic Address Table contains the MAC addresses learned by monitoring the source address for traffic entering the switch. When the destination address for inbound traffic is found in the database, the packets intended for that address are forwarded directly to the associated port. Otherwise, the traffic is flooded to all ports.

Command Attributes

- **Interface** – Indicates a port or trunk.
- **MAC Address** – Physical address associated with this interface.
- **VLAN** – ID of configured VLAN (1-4093).
- **Address Table Sort Key** – You can sort the information displayed based on MAC address, VLAN or interface (port or trunk).

Web – Click Address Table, Dynamic Addresses. Specify the search type (i.e., mark the Interface, MAC Address, or VLAN checkbox), select the method of sorting the displayed addresses, and then click Query.



Dynamic Addresses

Query by:		
☑ Interface	● Port 1	○ Trunk
□ MAC Address		
□ VLAN	1	
Address Table Sort Key	Address	

Dynamic Address Table	
Dynamic Address Counts	1
Current Dynamic Address Table	00-20-9C-23-CD-60, VLAN 2,Unit 1, Port 1, Dynamic

CLI – This example also displays the address table entries for port 1.

```
Console#show mac-address-table interface ethernet 1/1                   4-121
 Interface Mac Address       Vlan Type
 --------- ----------------- ---- -----------------
  Eth 1/ 1 00-E0-29-94-34-DE    1 Permanent
  Eth 1/ 1 00-20-9C-23-CD-60    2 Learned
Console#
```

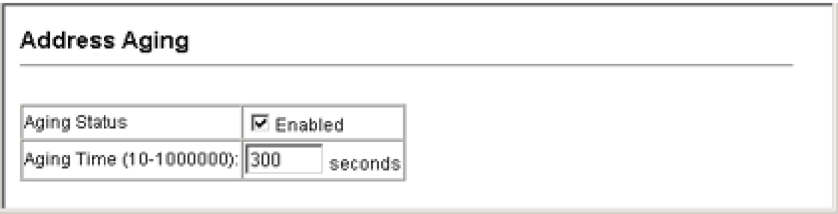
Changing the Aging Time

You can set the aging time for entries in the dynamic address table.

Command Attributes

- Aging Status – Enables/disables the function.
- Aging Time – The time after which a learned entry is discarded. (Range: 10-1000000 seconds; Default: 300 seconds)

Web – Click Address Table, Address Aging. Specify the new aging time, click Apply.



Address Aging

Aging Status	☑ Enabled
Aging Time (10-1000000):	300 seconds

CLI – This example sets the aging time to 400 seconds.

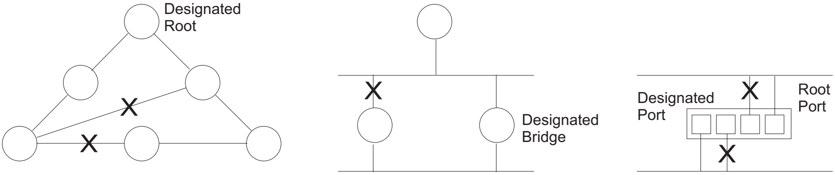
```
Console(config)#mac-address-table aging-time 400                        4-122
Console(config)#
```

Spanning Tree Algorithm Configuration

The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

The spanning tree algorithms supported by this switch include these versions:

- **STP** – Spanning Tree Protocol (IEEE 802.1D)
- **RSTP** – Rapid Spanning Tree Protocol (IEEE 802.1w) STA uses a distributed algorithm to select a bridging device (STA-compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. It selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. It then selects a port on the designated bridging device to communicate with each attached LAN or host device as a designated port. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.



Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge.

If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

RSTP is designed as a general replacement for the slower, legacy STP. RSTP achieves must faster reconfiguration (i.e., around one tenth of the time required by STP) by reducing the number of state changes before active ports start learning, predefining an alternate route that can be used when a node or port fails, and retaining the forwarding database for ports insensitive to changes in the tree structure when reconfiguration occurs.

Displaying Global Settings

You can display a summary of the current bridge STA information that applies to the entire switch using the STA Information screen.

Field Attributes

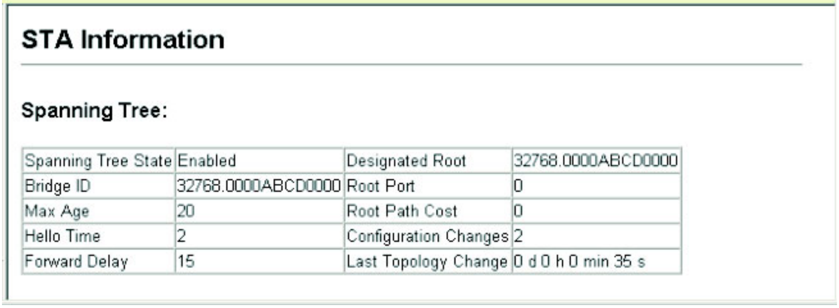
- **Spanning Tree State** – Shows if the switch is enabled to participate in an STA-compliant network.
- **Bridge ID** – A unique identifier for this bridge, consisting of the bridge priority and MAC address (where the address is taken from the switch system).
- **Max Age** – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. (References to “ports” in this section mean “interfaces,” which includes both ports and trunks.)
- **Hello Time** – Interval (in seconds) at which the root device transmits a configuration message.
- **Forward Delay** – The maximum time (in seconds) the root device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.
- **Designated Root** – The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device.
    - **Root Port** – The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the Spanning Tree network.
    - **Root Path Cost** – The path cost from the root port on this switch to the root device.
- **Configuration Changes** – The number of times the Spanning Tree has been reconfigured.
- **Last Topology Change** – Time since the Spanning Tree was last reconfigured.

These additional parameters are only displayed for the CLI:

- **Spanning tree mode** – Specifies the type of spanning tree used on this switch:
    - **STP**: Spanning Tree Protocol (IEEE 802.1D)
    - **RSTP**: Rapid Spanning Tree (IEEE 802.1w)
- **Priority** – Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.

- **Root Hello Time** – Interval (in seconds) at which this device transmits a configuration message.
- **Root Maximum Age** – The maximum time (in seconds) this device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. If the root port ages out STA information (provided in the last configuration message), a new root port is selected from among the device ports attached to the network. (References to “ports” in this section means “interfaces,” which includes both ports and trunks.)
- **Root Forward Delay** – The maximum time (in seconds) this device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.
- **Transmission limit** – The minimum interval between the transmission of consecutive RSTP BPDUs.
- **Path Cost Method** – The path cost is used to determine the best path between devices. The path cost method is used to determine the range of values that can be assigned to each interface.

Web – Click Spanning Tree, STA, Information.



STA Information

Spanning Tree:

Spanning Tree State	Enabled	Designated Root	32768.0000ABCD0000
Bridge ID	32768.0000ABCD0000	Root Port	0
Max Age	20	Root Path Cost	0
Hello Time	2	Configuration Changes	2
Forward Delay	15	Last Topology Change	0 d 0 h 0 min 35 s

CLI – This command displays global STA settings, followed by settings for each port.

```
Console#show spanning-tree                                           4-133
Spanning-tree information
---------------------------------------------------------------
 Spanning tree mode                :RSTP
 Spanning tree enable/disable      :enable
 Priority                          :32768
 Bridge Hello Time (sec.)          :2
 Bridge Max Age (sec.)             :20
 Bridge Forward Delay (sec.)       :15
 Root Hello Time (sec.)            :2
 Root Max Age (sec.)               :20
 Root Forward Delay (sec.)         :15
 Designated Root                   :32768.000087654321
 Current root port                 :1
 Current root cost                 :200000
 Number of topology changes        :1
 Last topology changes time (sec.):23771
 Transmission limit                :3
 Path Cost Method                  :long
.
.
.
```

Note: The current root port and current root cost display as zero when this device is not connected to the network.

Configuring Global Settings

Global settings apply to the entire switch.

Command Usage

- Spanning Tree Protocol

  Uses RSTP for the internal state machine, but sends only 802.1D BPDUs. Rapid Spanning Tree Protocol

- RSTP supports connections to either STP or RSTP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:
  - STP Mode – If the switch receives an 802.1D BPDU (i.e., STP BPDU) after a port’s migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.
  - RSTP Mode – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.

Command Attributes

Basic Configuration of Global Settings

- **Spanning Tree State** – Enables/disables STA on this switch. (Default: Enabled)
- **Spanning Tree Type** – Specifies the type of spanning tree used on this switch:
  - **STP**: Spanning Tree Protocol (IEEE 802.1D); i.e., when this option is selected, the switch will use RSTP set to STP forced compatibility mode).
  - **RSTP**: Rapid Spanning Tree (IEEE 802.1w); RSTP is the default.

- **Priority** – Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. (Note that lower numeric values indicate higher priority.)
  - Default: 32768
  - Range: 0-61440, in steps of 4096
  - Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440

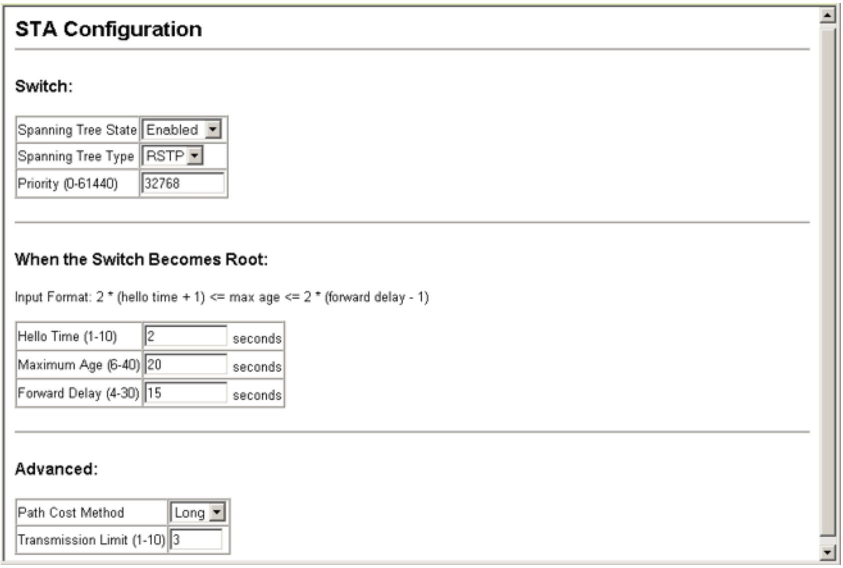
Root Device Configuration

- **Hello Time** – Interval (in seconds) at which the root device transmits a configuration message.
  - Default: 2
  - Minimum: 1
  - Maximum: The lower of 10 or [(Max. Message Age / 2) -1]
- **Maximum Age** – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. (References to “ports” in this section mean “interfaces,” which includes both ports and trunks.)
  - Default: 20
  - Minimum: The higher of 6 or [2 x (Hello Time + 1)].
  - Maximum: The lower of 40 or [2 x (Forward Delay - 1)]
- **Forward Delay** – The maximum time (in seconds) this device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.
  - Default: 15
  - Minimum: The higher of 4 or [(Max. Message Age / 2) + 1]
  - Maximum: 30

Configuration Settings for RSTP

- **Path Cost Method** – The path cost is used to determine the best path between devices. The path cost method is used to determine the range of values that can be assigned to each interface.
  - Long: Specifies 32-bit based values that range from 1-200,000,000. (This is the default.)
  - Short: Specifies 16-bit based values that range from 1-65535.
- **Transmission Limit** – The maximum transmission rate for BPDUs is specified by setting the minimum interval between the transmission of consecutive protocol messages. (Range: 1-10; Default: 3)

Web – Click Spanning Tree, STA, Configuration. Modify the required attributes, and click Apply.



STA Configuration

Switch:

Spanning Tree State	Enabled
Spanning Tree Type	RSTP
Priority (0-61440)	32768

When the Switch Becomes Root:

Input Format: 2 * (hello time + 1) <= max age <= 2 * (forward delay - 1)

Hello Time (1-10)	2	seconds
Maximum Age (6-40)	20	seconds
Forward Delay (4-30)	15	seconds

Advanced:

Path Cost Method	Long
Transmission Limit (1-10)	3

CLI – This example enables Spanning Tree Protocol, and then configures the STA parameters.

```
Console(config)#spanning-tree                                       4-124
Console(config)#spanning-tree priority 40000                        4-127
Console(config)#spanning-tree hello-time 5                          4-126
Console(config)#spanning-tree forward-time 20                       4-125
Console(config)#spanning-tree max-age 38                            4-126
Console(config)#spanning-tree pathcost method long                  4-128
Console(config)#spanning-tree transmission-limit 4                  4-128
```

Displaying Interface Settings

The STA Port Information and STA Trunk Information pages display the current status of ports and trunks in the Spanning Tree.

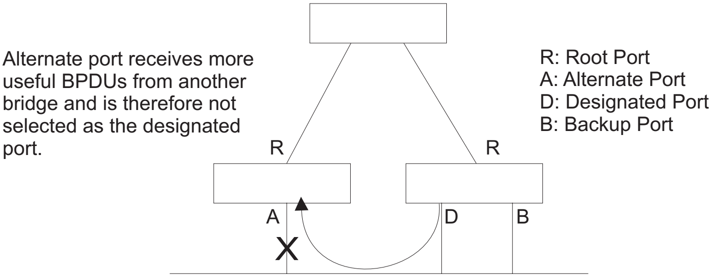
Command Attributes

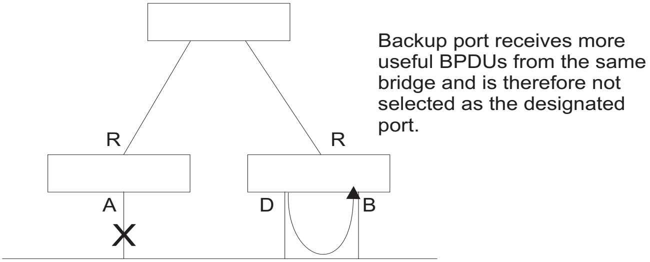
- **Spanning Tree** – Shows if STA has been enabled on this interface.
- **STA Status** – Displays current state of this port within the Spanning Tree:
  - **Discarding** - Port receives STA configuration messages but does not forward packets.
  - **Learning** - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
  - **Forwarding** - Port forwards packets, and continues learning addresses.

The rules defining port status are:

- A port on a network segment with no other STA compliant bridging device is always forwarding.
- If two ports of a switch are connected to the same segment and there is no other STA device attached to this segment, the port with the smaller ID forwards packets and the other is discarding.
- All ports are discarding when the switch is booted, then some of them change state to learning, and then to forwarding.

- **Forward Transitions** – The number of times this port has transitioned from the Learning state to the Forwarding state.
- **Designated Cos**t – The cost for a packet to travel from this port to the root in the current Spanning Tree configuration. The slower the media, the higher the cost.
- **Designated Bridge** – The bridge priority and MAC address of the device through which this port must communicate to reach the root of the Spanning Tree.
- **Designated Port** – The port priority and number of the port on the designated bridging device through which this switch must communicate with the root of the Spanning Tree.
- **Oper Link Type** – The operational point-to-point status of the LAN segment attached to this interface. This parameter is determined by manual configuration or by auto-detection, as described for Admin Link Type in STA Port Configuration on page 3-81.
- **Oper Edge Port** – This parameter is initialized to the setting for Admin Edge Port in STA Port Configuration on page 3-81 (i.e., true or false), but will be set to false if a BPDU is received, indicating that another bridge is attached to this port.
- **Port Role** – Roles are assigned according to whether the port is part of the active topology connecting the bridge to the root bridge (i.e., root port), connecting a LAN through the bridge to the root bridge (i.e., designated port); or is an alternate or backup port that may provide connectivity if other bridges, bridge ports, or LANs fail or are removed. The role is set to disabled (i.e., disabled port) if a port has no role within the spanning tree.
- **Trunk Member** – Indicates if a port is a member of a trunk. (STA Port Information only)

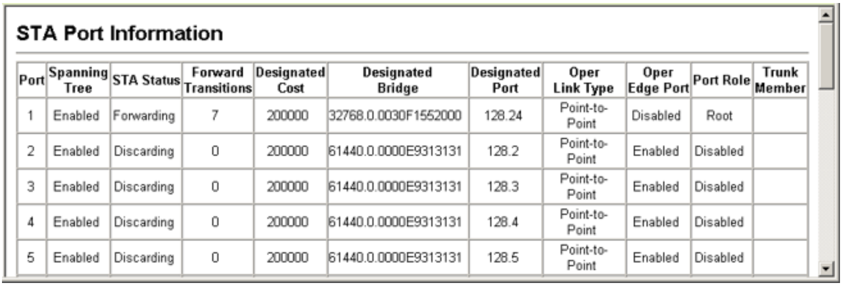

Alternate port receives more useful BPDUs from another bridge and is therefore not selected as the designated port.
R: Root Port
A: Alternate Port
D: Designated Port
B: Backup Port
R
R
A
D
B
X


Backup port receives more useful BPDUs from the same bridge and is therefore not selected as the designated port.
R
R
A
X
D
B

These additional parameters are only displayed for the CLI:

- **Admin status** – Shows if this interface is enabled.
- Path Cost – This parameter is used by the STA to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.)
- **Designated root** – The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device.
- **Fast forwarding** – This field provides the same information as Admin Edge port, and is only included for backward compatibility with earlier products.
- **Admin Edge Port** – You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to reconfigure when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device.
- **Admin Link Type** – The link type attached to this interface.
  - Point-to-Point – A connection to exactly one other bridge.
  - Shared – A connection to two or more bridges.
  - Auto – The switch automatically determines if the interface is attached to a point-to-point link or to shared media.

Web – Click Spanning Tree, STA, Port Information or STA Trunk Information.



STA Port Information

Port	Spanning Tree	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Link Type	Oper Edge Port	Port Role	Trunk Member
1	Enabled	Forwarding	7	200000	32768.0.0030F1552000	128.24	Point-to-Point	Disabled	Root	
2	Enabled	Discarding	0	200000	61440.0.0000E9313131	128.2	Point-to-Point	Enabled	Disabled	
3	Enabled	Discarding	0	200000	61440.0.0000E9313131	128.3	Point-to-Point	Enabled	Disabled	
4	Enabled	Discarding	0	200000	61440.0.0000E9313131	128.4	Point-to-Point	Enabled	Disabled	
5	Enabled	Discarding	0	200000	61440.0.0000E9313131	128.5	Point-to-Point	Enabled	Disabled	

CLI – This example shows the STA attributes for port 5.

```
Console#show spanning-tree ethernet 1/5                                4-133
Eth  1/ 5 information
-------------------------------------------------------------
 Admin status          : enable
 Role                  : disable
 State                 : discarding
 Path cost             : 100000
 Priority              : 128
 Designated cost       : 200000
 Designated port       : 128.5
 Designated root       : 61440.0.0000E9313131
 Designated bridge     : 61440.0.0000E9313131
 Fast forwarding       : enable
 Forward transitions   : 0
 Admin edge port       : enable
 Oper edge port        : enable
 Admin Link type       : auto
 Oper Link type        : point-to-point
 Spanning Tree Status  : enable
```

Configuring Interface Settings

You can configure RSTP attributes for specific interfaces, including port priority, path cost, link type, and edge port. You may use a different priority or path cost for ports of the same media type to indicate the preferred path, link type to indicate a point-to-point connection or shared-media connection, and edge port to indicate if the attached device can support fast forwarding.

Command Attributes

The following attributes are read-only and cannot be changed:

- **STA State** – Displays current state of this port within the Spanning Tree. (See “Displaying Interface Settings” on page 3-78 for additional information.)
  - **Discarding** - Port receives STA configuration messages but does not forward packets.
  - **Learning** - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
  - **Forwarding** - Port forwards packets, and continues learning addresses.

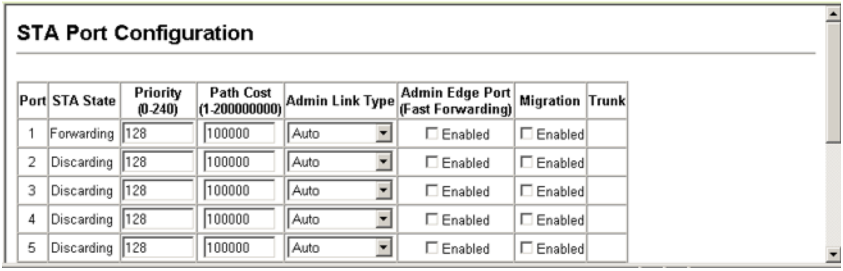
- **Trunk** – Indicates if a port is a member of a trunk.
  (STA Port Configuration only)

The following interface attributes can be configured:

- **Priority** – Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.
  - Default: 128
  - Range: 0-240, in steps of 16
- **Path Cost** – This parameter is used by the STP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.) Note that when the Path Cost Method is set to short (page 3-63), the maximum path cost is 65,535.
  - Range
    - Ethernet: 200,000-20,000,000
    - Fast Ethernet: 20,000-2,000,000
    - Gigabit Ethernet: 2,000-200,000
  - Default
    - Ethernet – Half duplex: 2,000,000; full duplex: 1,000,000; trunk: 500,000
    - Fast Ethernet – Half duplex: 200,000; full duplex: 100,000; trunk: 50,000
    - Gigabit Ethernet – Full duplex: 10,000; trunk: 5,000
- **Admin Link Type** – The link type attached to this interface.
  - Point-to-Point – A connection to exactly one other bridge.
  - Shared – A connection to two or more bridges.
  - Auto – The switch automatically determines if the interface is attached to a point-to-point link or to shared media. (This is the default setting.)
- **Admin Edge Port (Fast Forwarding)** – You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device. (Default: Disabled)

- **Migration** – If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the Protocol Migration button to manually re-check the appropriate BPDU format (RSTP or STP-compatible) to send on the selected interfaces. (Default: Disabled)

Web – Click Spanning Tree, STA, Port Configuration or Trunk Configuration. Modify the required attributes, then click Apply.



STA Port Configuration

Port	STA State	Priority (0-240)	Path Cost (1-200000000)	Admin Link Type	Admin Edge Port (Fast Forwarding)	Migration	Trunk
1	Forwarding	128	100000	Auto	□ Enabled	□ Enabled	
2	Discarding	128	100000	Auto	□ Enabled	□ Enabled	
3	Discarding	128	100000	Auto	□ Enabled	□ Enabled	
4	Discarding	128	100000	Auto	□ Enabled	□ Enabled	
5	Discarding	128	100000	Auto	□ Enabled	□ Enabled	

CLI – This example sets STA attributes for port 7.

```
Console(config)#interface ethernet 1/7                                4-86
Console(config-if)#spanning-tree port-priority 0                      4-127
Console(config-if)#spanning-tree cost 50                              4-129
Console(config-if)#spanning-tree link-type auto                       4-132
Console(config-if)#no spanning-tree edge-port                         4-130
Console(config-if)#spanning-tree protocol-migration                   4-133
Console(config-if)#
```

VLAN Configuration

Overview

In large networks, routers are used to isolate broadcast traffic for each subnet into separate domains. This switch provides a similar service at Layer 2 by using VLANs to organize any group of network nodes into separate broadcast domains. VLANs confine broadcast traffic to the originating group, and can eliminate broadcast storms in large networks. This also provides a more secure and cleaner network environment.

An IEEE 802.1Q VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment.

VLANs help to simplify network management by allowing you to move devices to a new VLAN without having to change any physical connections. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as videoconferencing).

VLANs provide greater network efficiency by reducing broadcast traffic, and allow you to make network changes without having to update IP addresses or IP subnets. VLANs inherently provide a high level of network security since traffic must pass through a configured Layer 3 link to reach a different VLAN.

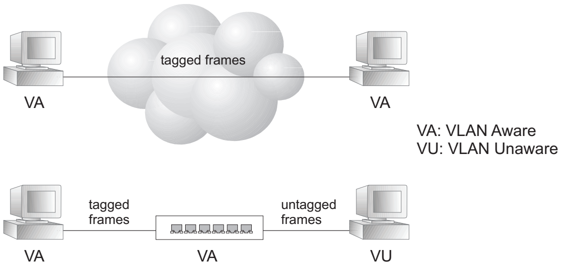
This switch supports the following VLAN features:

- Up to 255 VLANs based on the IEEE 802.1Q standard
- Distributed VLAN learning across multiple switches using explicit or implicit tagging
- Port overlapping, allowing a port to participate in multiple VLANs
- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware and VLAN-unaware devices
- Priority tagging

Assigning Ports to VLANs

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) in which it will participate. By default all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port if you want it to carry traffic for one or more VLANs, and any intermediate network devices or the host at the other end of the connection supports VLANs. Then manually assign ports on the other VLAN-aware network devices along the path that will carry this traffic to the same VLAN(s). However, if you want a port on this switch to participate in one or more VLANs, but none of the intermediate network devices nor the host at the other end of the connection supports VLANs, then you should add this port to the VLAN as an untagged port.

Note: VLAN-tagged frames can pass through VLAN-aware or VLAN-unaware network interconnection devices, but the VLAN tags should be stripped off before passing it on to any end-node host that does not support VLAN tagging.



VLAN Classification – When the switch receives a frame, it classifies the frame in one of two ways. If the frame is untagged, the switch assigns the frame to an associated VLAN (based on the default VLAN ID of the receiving port). But if the frame is tagged, the switch uses the tagged VLAN ID to identify the port broadcast domain of the frame.

Port Overlapping – Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if you implement VLANs which do not overlap, but still need to communicate, you can connect them by enabled routing on this switch.

Untagged VLANs – Untagged (or static) VLANs are typically used to reduce broadcast traffic and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other VLANs configured on the switch. Packets are forwarded only between ports that are designated for the same VLAN. Untagged VLANs can be used to manually isolate user groups or subnets.

Forwarding Tagged/Untagged Frames

If you want to create a small port-based VLAN for devices attached directly to a single switch, you can assign ports to the same untagged VLAN. However, to participate in a VLAN group that crosses several switches, you should create a VLAN for that group and enable tagging on all ports.

Ports can be assigned to multiple tagged or untagged VLANs. Each port on the switch is therefore capable of passing tagged or untagged frames. When forwarding a frame from this switch along a path that contains any VLAN-aware devices, the switch should include VLAN tags. When forwarding a frame from this switch along a path that does not contain any VLAN-aware devices (including the destination host), the switch must first strip off the VLAN tag before forwarding the frame. When the switch receives a tagged frame, it will pass this frame onto the VLAN(s) indicated by the frame tag. However, when this switch receives an untagged frame from a VLAN-unaware device, it first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port’s default VID.

Displaying Basic VLAN Information

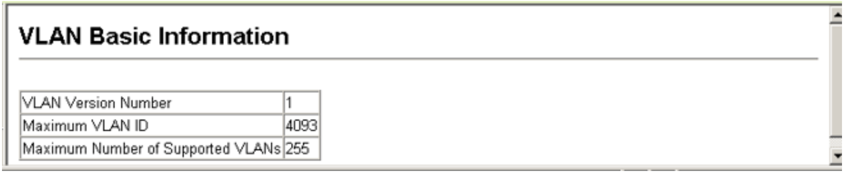
The VLAN Basic Information page displays basic information on the VLAN type supported by the switch.

Field Attributes

- **VLAN Version Number*** – The VLAN version used by this switch as specified in the IEEE 802.1Q standard.
- **Maximum VLAN ID** – Maximum VLAN ID recognized by this switch.
- **Maximum Number of Supported VLANs** – Maximum number of VLANs that can be configured on this switch.

* Web Only

Web – Click VLAN, 802.1Q VLAN, Basic Information.



VLAN Basic Information

VLAN Version Number	1
Maximum VLAN ID	4093
Maximum Number of Supported VLANs	255

CLI – Enter the following command.

```
Console#show bridge-ext                                                  4-144
 Max support vlan numbers: 255
 Max support vlan ID: 4093
 Extended multicast filtering services: No
 Static entry individual port: Yes
 VLAN learning: IVL
 Configurable PVID tagging: Yes
 Local VLAN capable: No
 Traffic classes: Enabled
 GMRP: Disabled
Console#
```

Displaying Current VLANs

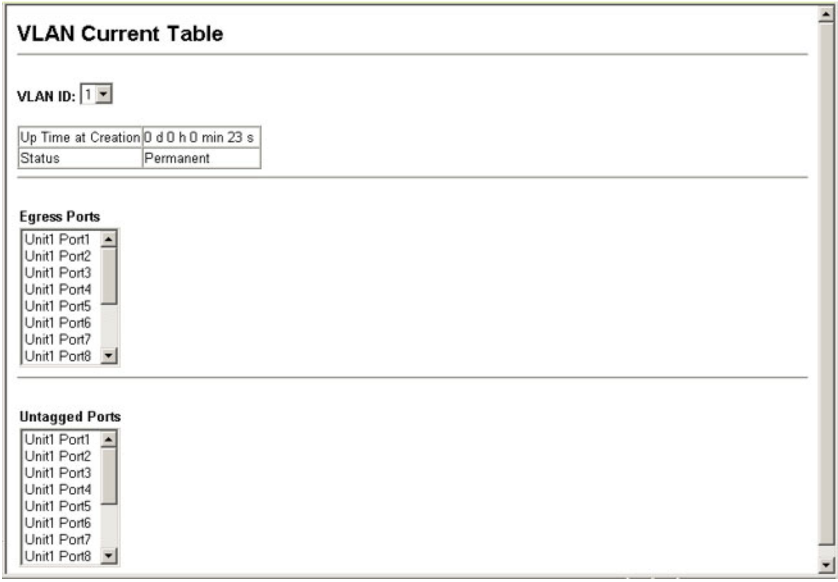
The VLAN Current Table shows the current port members of each VLAN and whether or not the port supports VLAN tagging. Ports assigned to a large VLAN group that crosses several switches should use VLAN tagging. However, if you just want to create a small port-based VLAN for one or two switches, you can disable tagging.

Command Attributes (Web)

- **VLAN ID** – ID of configured VLAN (1-4093)
- **Up Time at Creation** – Time this VLAN was created (i.e., System Up Time)
- **Status** – Shows how this VLAN was added to the switch
  - **Dynamic GVRP:** Automatically learned via GVRP*
  - **Permanent:** Added as a static entry
- **Egress Ports** – Shows all the VLAN port members
- **Untagged Ports** – Shows the untagged VLAN port members

* Not supported in the current version

Web – Click VLAN, 802.1Q VLAN, Current Table. Select any ID from the scroll-down list.



VLAN Current Table

VLAN ID: 1

Up Time at Creation	0 d 0 h 0 min 23 s
Status	Permanent

Egress Ports

Unit1 Port1
Unit1 Port2
Unit1 Port3
Unit1 Port4
Unit1 Port5
Unit1 Port6
Unit1 Port7
Unit1 Port8

Untagged Ports

Unit1 Port1
Unit1 Port2
Unit1 Port3
Unit1 Port4
Unit1 Port5
Unit1 Port6
Unit1 Port7
Unit1 Port8

Command Attributes (CLI)

- **VLAN** – ID of configured VLAN (1-4094, no leading zeroes)
- **Type** – Shows how this VLAN was added to the switch
  - **Dynamic:** Automatically learned via GVRP*
  - **Static:** Added as a static entry

* Not supported in the current version

- **Name** – Name of the VLAN (1 to 32 characters)
- **Status** – Shows if this VLAN is enabled or disabled
  - **Active:** VLAN is operational
  - **Suspend:** VLAN is suspended; i.e., does not pass packets
- **Ports / Channel groups** – Shows the VLAN interface members

CLI – Current VLAN information can be displayed with the following command.

```
Console#show vlan id 1                                                   4-141
VLAN Type    Name              Status    Ports/Channel groups
---- ------- ---------------- --------- ----------------------------------------
   1  Static      DefaultVlan    Active Eth1/ 1 Eth1/ 2 Eth1/ 3 Eth1/ 4 Eth1/ 5
                                        Eth1/ 6 Eth1/ 7 Eth1/ 8 Eth1/ 9 Eth1/10
                                        Eth1/11 Eth1/12 Eth1/13 Eth1/14
Console#
```

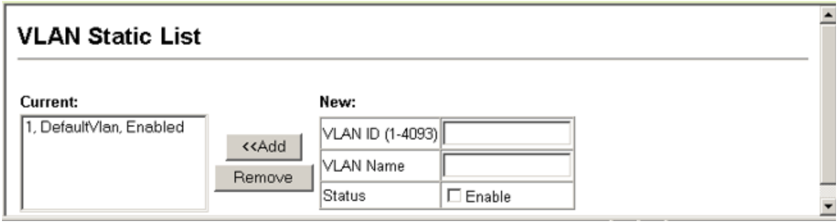
Creating VLANs

Use the VLAN Static List to create or remove VLAN groups. To propagate information about VLAN groups used on this switch to external network devices, you must specify a VLAN ID for each of these groups.

Command Attributes

- **Current** – Lists all the current VLAN groups created for this system. Up to 255 VLAN groups can be defined. VLAN 1 is the default untagged VLAN.
- **New** – Allows you to specify the name and numeric identifier for a new VLAN group. (The VLAN name is only used for management on this system; it is not added to the VLAN tag.)
- **VLAN ID** – ID of configured VLAN (1-4093, no leading zeroes).
- **VLAN Name** – Name of the VLAN (1 to 32 characters).
- **Status (Web)** – Enables or disables the specified VLAN.
  - **Enable:** VLAN is operational.
  - **Disable:** VLAN is suspended; i.e., does not pass packets.
- **State (CLI)** – Enables or disables the specified VLAN.
  - **Active:** VLAN is operational.
  - **Suspend:** VLAN is suspended; i.e., does not pass packets.
- **Add** – Adds a new VLAN group to the current list.
- **Remove** – Removes a VLAN group from the current list. If any port is assigned to this group as untagged, it will be reassigned to VLAN group 1 as untagged.

Web – Click VLAN, 802.1Q VLAN, Static List. To create a new VLAN, enter the VLAN ID and VLAN name, mark the Enable checkbox to activate the VLAN, and then click Add.



VLAN Static List

Current:

1, DefaultVlan, Enabled

New:

VLAN ID (1-4093)	
VLAN Name	
Status	□ Enable

CLI – This example creates a new VLAN.

```
Console(config)#vlan database                                         4-135
Console(config-vlan)#vlan 2 name R&D media ethernet state active      4-136
Console(config-vlan)#end
Console#show vlan                                                     4-141
VLAN Type    Name             Status    Ports/Channel groups
---- ------- ---------------- --------- ----------------------------------
   1  Static      DefaultVlan    Active Eth1/ 1 Eth1/ 2 Eth1/ 3 Eth1/ 4 Eth1/ 5
                                        Eth1/ 6 Eth1/ 7 Eth1/ 8 Eth1/ 9 Eth1/10
                                        Eth1/11 Eth1/12 Eth1/13 Eth1/14 Eth1/15
                                        Eth1/16 Eth1/17 Eth1/18 Eth1/19 Eth1/20
                                        Eth1/21 Eth1/22 Eth1/23 Eth1/24
   2  Static              R&D    Active
Console(config-vlan)#
```

Adding Static Members to VLANs (VLAN Index)

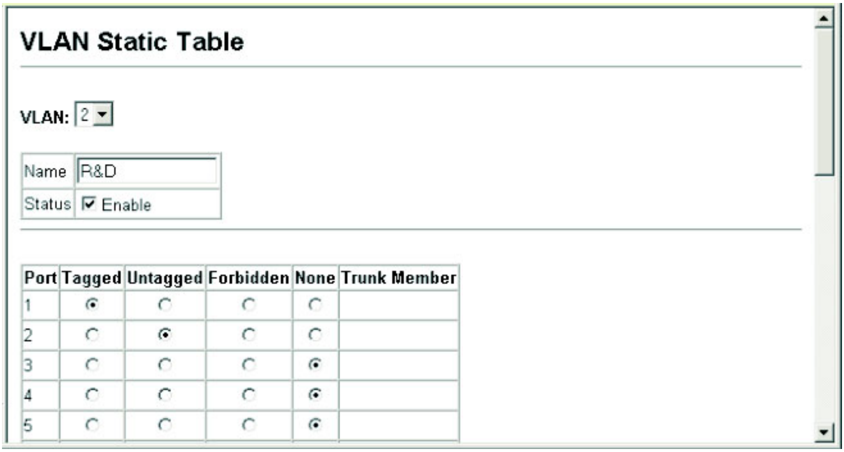
Notes: **1.** Use the VLAN Static Table to configure port members for the selected VLAN index. Assign ports as tagged if they are connected to 802.1Q VLAN compliant devices, or untagged they are not connected to any VLAN-aware devices.You can also use the VLAN Static Membership by Port page to configure VLAN groups based on the port index (page 3-90). However, note that this configuration page can only add ports to a VLAN as tagged members.

2. VLAN 1 is the default untagged VLAN containing all ports on the switch, and can only be modified by first reassigning the default port VLAN ID as described under “Configuring VLAN Behavior for Interfaces” on page 3-91.

Command Attributes

- **VLAN** – ID of configured VLAN (1-4094, no leading zeroes).
- **Name** – Name of the VLAN (1 to 32 characters).
- **Status** – Enables or disables the specified VLAN.
  - **Enable**: VLAN is operational.
  - **Disable**: VLAN is suspended; i.e., does not pass packets.
- **Port** – Port identifier.
- **Trunk** – Trunk identifier.
- **Membership Type** – Select VLAN membership for each interface by marking the appropriate radio button for a port or trunk:
  - **Tagged**: Interface is a member of the VLAN. All packets transmitted by the port will be tagged, that is, carry a tag and therefore carry VLAN or CoS information.
  - **Untagged**: Interface is a member of the VLAN. All packets transmitted by the port will be untagged, that is, not carry a tag and therefore not carry VLAN or CoS information. Note that an interface must be assigned to at least one group as an untagged port.
  - **None**: Interface is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the interface.
- **Trunk Member** – Indicates if a port is a member of a trunk. To add a trunk to the selected VLAN, use the last table on the VLAN Static Table page.

Web – Click VLAN, 802.1Q VLAN, Static Table. Select a VLAN ID from the scroll-down list. Modify the VLAN name and status if required. Select the membership type by marking the appropriate radio button in the list of ports or trunks. Click Apply.



VLAN Static Table

VLAN: 2

Name	R&D
Status	☑ Enable

Port	Tagged	Untagged	Forbidden	None	Trunk Member
1	●	○	○	○	
2	○	●	○	○	
3	○	○	○	●	
4	○	○	○	●	
5	○	○	○	●	

CLI – The following example adds tagged and untagged ports to VLAN 2.

```
Console(config)#interface ethernet 1/1                                    4-86
Console(config-if)#switchport allowed vlan add 2 tagged                   4-140
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#switchport allowed vlan add 2 untagged
Console(config-if)#exit
Console(config)#interface ethernet 1/13
Console(config-if)#switchport allowed vlan add 2 tagged
```

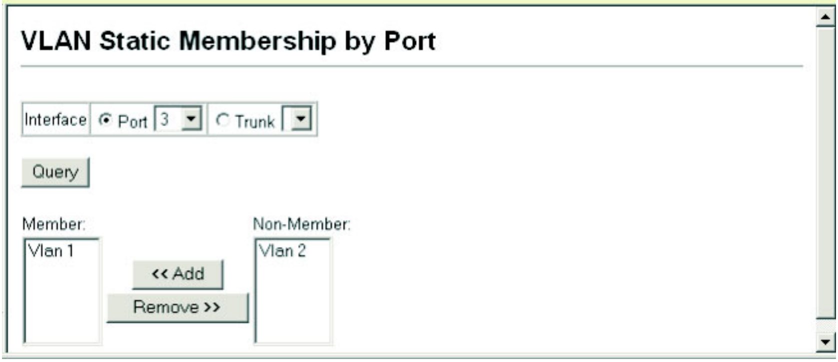
Adding Static Members to VLANs (Port Index)

Use the VLAN Static Membership by Port menu to assign VLAN groups to the selected interface as a tagged member.

Command Attributes

- **Interface** – Port or trunk identifier.
- **Member** – VLANs for which the selected interface is a tagged member.
- **Non-Member** – VLANs for which the selected interface is not a tagged member.

Web – Open VLAN, 802.1Q VLAN, Static Membership. Select an interface from the scroll-down box (Port or Trunk). Click Query to display membership information for the interface. Select a VLAN ID, and then click Add to add the interface as a tagged member, or click Remove to remove the interface. After configuring VLAN membership for each interface, click Apply.



VLAN Static Membership by Port

Interface ● Port 3 ○ Trunk

Member: Vlan 1

Non-Member: Vlan 2

CLI – This example adds Port 3 to VLAN 1 as a tagged port, and removes Port 3 from VLAN 2.

```
Console(config)#interface ethernet 1/3                        4-86
Console(config-if)#switchport allowed vlan add 1 tagged       4-140
Console(config-if)#switchport allowed vlan remove 2
```

Configuring VLAN Behavior for Interfaces

You can configure VLAN behavior for specific interfaces, including the default VLAN identifier (PVID), accepted frame types, and ingress filtering.

Command Attributes

- **PVID** – VLAN ID assigned to untagged frames received on the interface. (Default: 1)

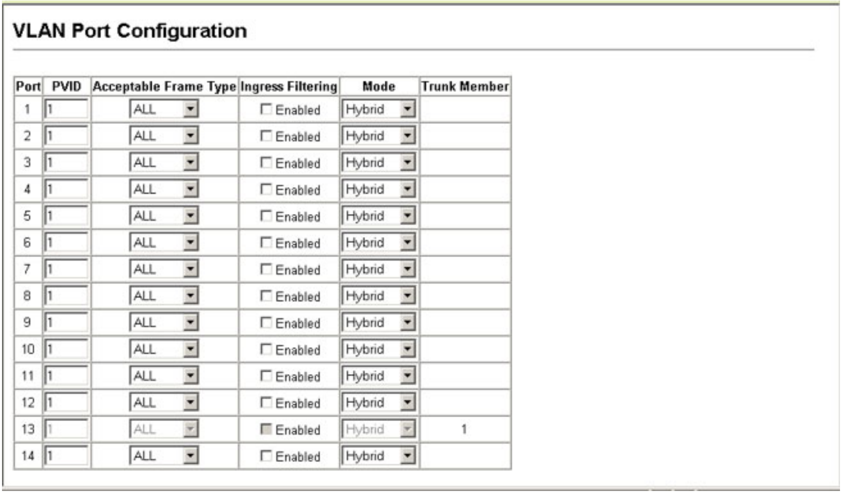
  If an interface is not a member of VLAN 1 and you assign its PVID to this VLAN, the interface will automatically be added to VLAN 1 as an untagged member. For all other VLANs, an interface must first be configured as an untagged member before you can assign its PVID to that group.

- **Acceptable Frame Type** – Sets the interface to accept all frame types, including tagged or untagged frames, or only tagged frames. When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN. (Option: All, Tagged; Default: All)

- **Ingress Filtering** – Determines how to process frames tagged for VLANs for which the ingress port is not a member. (Default: Disabled)
  - Ingress filtering only affects tagged frames.
  - If ingress filtering is disabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be flooded to all other ports (except for those VLANs explicitly forbidden on this port).
  - If ingress filtering is enabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be discarded.
  - Ingress filtering does not affect VLAN independent BPDU frames, such as STP. However, they do affect VLAN dependent BPDU frames, such as GMRP.
- **GARP Join Time**r* – The interval between transmitting requests/queries to participate in a VLAN group. (Range: 20-1000 centiseconds; Default: 20)
- **GARP Leave Time**r* – The interval a port waits before leaving a VLAN group. This time should be set to more than twice the join time. This ensures that after a Leave or LeaveAll message has been issued, the applicants can rejoin before the port actually leaves the group. (Range: 60-3000 centiseconds; Default: 60)
- **GARP LeaveAll Timer*** – The interval between sending out a LeaveAll query message for VLAN group participants and the port leaving the group. This interval should be considerably larger than the Leave Time to minimize the amount of traffic generated by nodes rejoining the group.
  (Range: 500-18000 centiseconds; Default: 1000)
- **Mode** – Indicates VLAN membership mode for an interface. (Default: 1Q Trunk)
  - **1Q Trunk** – Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. However, note that frames belonging to the port's default VLAN (i.e., associated with the PVID) are sent untagged.
  - **Hybrid** – Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.
- Trunk Member – Indicates if a port is a member of a trunk. To add a trunk to the selected VLAN, use the last table on the VLAN Static Table page.

* Timer settings must follow this rule: 2 x (join timer) < leave timer < leaveAll timer

Web – Click VLAN, 802.1Q VLAN, Port Configuration or VLAN Trunk Configuration. Fill in the required settings for each interface, click Apply.



VLAN Port Configuration

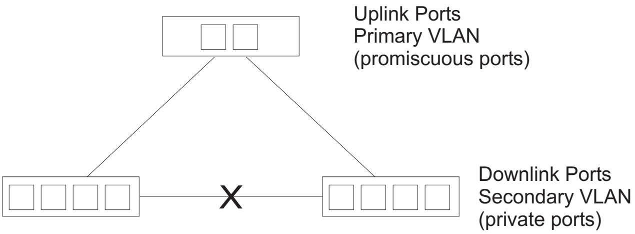
Port	PVID	Acceptable Frame Type	Ingress Filtering	Mode	Trunk Member
1	1	ALL	□ Enabled	Hybrid	
2	1	ALL	□ Enabled	Hybrid	
3	1	ALL	□ Enabled	Hybrid	
4	1	ALL	□ Enabled	Hybrid	
5	1	ALL	□ Enabled	Hybrid	
6	1	ALL	□ Enabled	Hybrid	
7	1	ALL	□ Enabled	Hybrid	
8	1	ALL	□ Enabled	Hybrid	
9	1	ALL	□ Enabled	Hybrid	
10	1	ALL	□ Enabled	Hybrid	
11	1	ALL	□ Enabled	Hybrid	
12	1	ALL	□ Enabled	Hybrid	
13	1	ALL	□ Enabled	Hybrid	1
14	1	ALL	□ Enabled	Hybrid	

CLI – This example sets port 3 to accept only tagged frames, assigns PVID 3 as the native VLAN ID, sets the GARP timers, and then sets the switchport mode to hybrid.

```
Console(config)#interface ethernet 1/3                              4-86
Console(config-if)#switchport acceptable-frame-types tagged         4-138
Console(config-if)#switchport ingress-filtering                     4-139
Console(config-if)#switchport native vlan 3                         4-140
Console(config-if)#switchport mode hybrid                           4-138
Console(config-if)#
```

Configuring Private VLANs

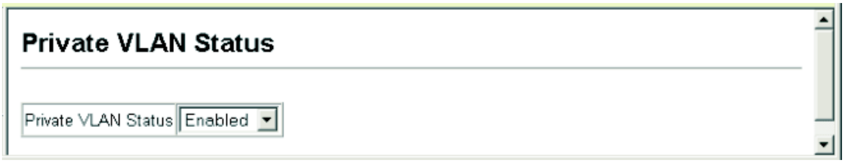
Private VLANs provide port-based security and isolation between ports within the assigned VLAN. Data traffic on downlink ports can only be forwarded to, and from, uplink ports. (Note that private VLANs and normal VLANs can exist simultaneously within the same switch.)



Enabling Private VLANs

Use the Private VLAN Status page to enable/disable the Private VLAN function.

Web – Click VLAN, Private VLAN, Status. Select Enable or Disable from the scroll-down box, and click Apply.



Private VLAN Status

Private VLAN Status: Enabled

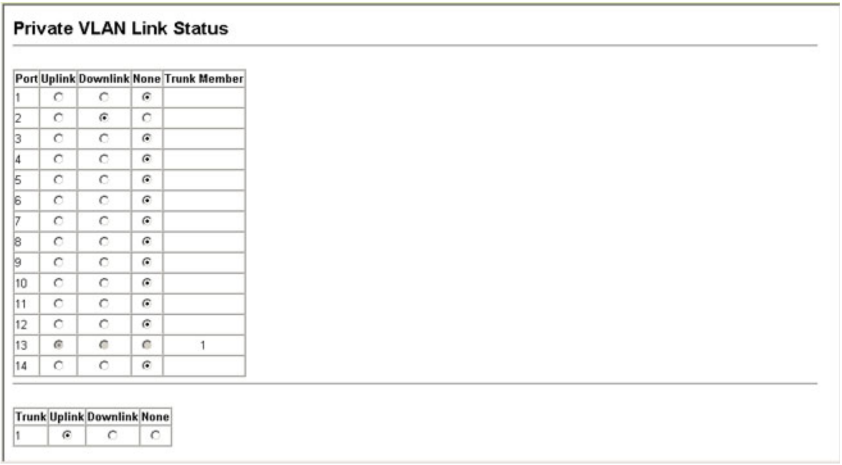
CLI – This example enables private VLANs.

```
Console(config)#pvlan                                          4-142
Console(config)#
```

Configuring Uplink and Downlink Ports

Use the Private VLAN Link Status page to set ports as downlink or uplink ports. Ports designated as downlink ports can not communicate with any other ports on the switch except for the uplink ports. Uplink ports can communicate with any other ports on the switch and with any designated downlink ports.

Web – Click VLAN, Private VLAN, Link Status. Check the ports that will serve as uplinks and downlinks for the private VLAN, then click Apply.



Private VLAN Link Status

Port	Uplink	Downlink	None	Trunk Member
1	○	○	●	
2	○	●	○	
3	○	○	●	
4	○	○	●	
5	○	○	●	
6	○	○	●	
7	○	○	●	
8	○	○	●	
9	○	○	●	
10	○	○	●	
11	○	○	●	
12	○	○	●	
13	●	○	○	1
14	○	○	●	

Trunk	Uplink	Downlink	None
1	●	○	○

CLI – This example configures ports 13 and 14 as uplink ports and ports 1-8 as downlink ports.

```
Console(config)#Console(config)#pvlan up-link ethernet 1/13-14 down-link
ethernet 1/1-8                                                      4-142
Console(config)#end
Console#show pvlan
Private VLAN status: Enabled
Up-link port:
 Ethernet 1/13
 Ethernet 1/14
Down-link port:
 Ethernet 1/1
 Ethernet 1/2
 Ethernet 1/3
 Ethernet 1/4
 Ethernet 1/5
 Ethernet 1/6
 Ethernet 1/7
 Ethernet 1/8
Console#
Console(config)#
```

Class of Service Configuration

Class of Service (CoS) allows you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with four priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. You can set the default priority for each interface, and configure the mapping of frame priority tags to the switch's priority queues.

Setting the Default Priority for Interfaces

You can specify the default port priority for each interface on the switch. All untagged packets entering the switch are tagged with the specified default port priority, and then sorted into the appropriate priority queue at the output port.

Command Usage

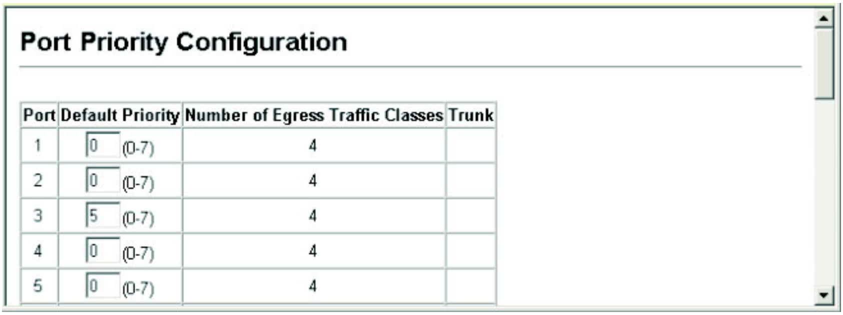
- This switch provides four priority queues for each port. It uses Weighted Round Robin to prevent head-of-queue blockage.
- The default priority applies for an untagged frame received on a port set to accept all frame types (i.e, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.
- If the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.

Command Attributes

- Default Priority* – The priority that is assigned to untagged frames received on the specified interface. (Range: 0 - 7, Default: 0)
- Number of Egress Traffic Classes – The number of queue buffers provided for each port.

* CLI displays this information as "Priority for untagged traffic."

Web – Click Priority, Default Port Priority or Default Trunk Priority. Modify the default priority for any interface, then click Apply.



Port Priority Configuration

Port	Default Priority	Number of Egress Traffic Classes	Trunk
1	0 (0-7)	4	
2	0 (0-7)	4	
3	5 (0-7)	4	
4	0 (0-7)	4	
5	0 (0-7)	4	

CLI – This example assigns a default priority of 5 to port 3.

```
Console(config)#interface ethernet 1/3                                      4-86
Console(config-if)#switchport priority default 5                            4-145
Console(config-if)#end
Console#show interfaces switchport ethernet 1/5                             4-95
Information of Eth 1/5
 Broadcast threshold: Enabled, 500 packets/second
 Lacp status: Disabled
 Ingress rate limit: disable,100M bits per second
 Egress rate limit: disable,100M bits per second
 VLAN membership mode: Hybrid
 Ingress rule: Disabled
 Acceptable frame type: All frames
 Native VLAN: 1
 Priority for untagged traffic: 0
 Gvrp status: Disabled*
 Allowed Vlan:    1(u),
 Forbidden Vlan:
Console#
```

* Not supported in the current version

Mapping CoS Values to Egress Queues

This switch processes Class of Service (CoS) priority tagged traffic by using four priority queues for each port, with service schedules based on strict or Weighted Round Robin (WRR). Up to eight separate traffic priorities are defined in IEEE 802.1p. The default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown in the following table.

Queue	0	1	2	3
Priority	1, 2	0, 3	4, 5	6, 7

The priority levels recommended in the IEEE 802.1p standard for various network applications are shown in the following table. However, you can map the priority levels to the switch's output queues in any way that benefits application traffic for your own network.

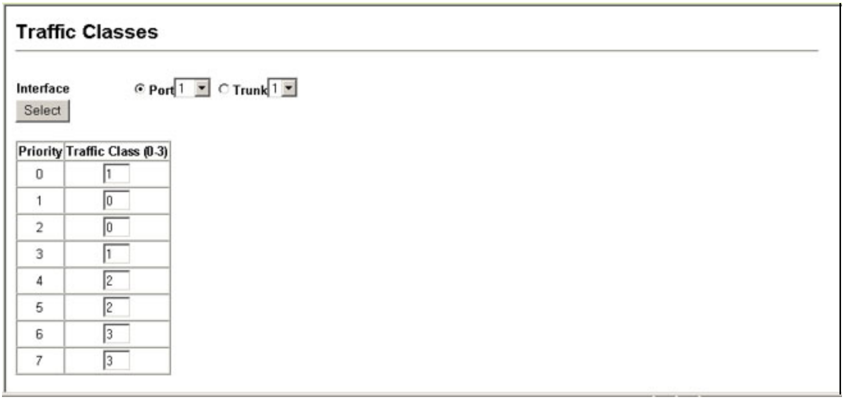
Priority Level	Traffic Type
1	Background
2	(Spare)
0 (default)	Best Effort
3	Excellent Effort
4	Controlled Load
5	Video, less than 100 milliseconds latency and jitter
6	Voice, less than 10 milliseconds latency and jitter
7	Network Control

Command Attributes

- **Priority** – CoS value. (Range: 0-7, where 7 is the highest priority)
- **Traffic Class*** – Output queue buffer. (Range: 0-3, where 3 is the highest CoS priority queue)

* CLI shows Queue ID

Web – Click Priority, Traffic Classes. Mark an interface and click Select to display the current mapping of CoS values to output queues. Assign priorities to the traffic classes (i.e., output queues) for the selected interface, then click Apply.



Traffic Classes

Interface ● Port 1 ○ Trunk 1

Priority	Traffic Class (0-3)
0	1
1	0
2	0
3	1
4	2
5	2
6	3
7	3

CLI – The following example shows how to change the CoS assignments to a one-to-one mapping.

```
Console(config)#interface ethernet 1/1                                    4-86
Console(config)#queue cos-map 0 0                                         4-148
Console(config)#queue cos-map 1 1
Console(config)#queue cos-map 2 2
Console(config)#exit
Console#show queue cos-map ethernet 1/1                                   4-149
Information of Eth 1/1
 Traffic Class : 0 1 2 3 4 5 6 7
 Priority Queue: 0 1 2 1 2 2 3 3
```

* Mapping specific values for CoS priorities is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

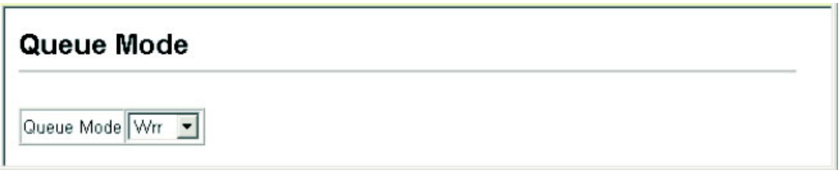
Selecting the Queue Mode

You can set the switch to service the queues based on a strict rule that requires all traffic in a higher priority queue to be processed before lower priority queues are serviced, or use Weighted Round-Robin (WRR) queuing that specifies a relative weight of each queue. WRR uses a predefined relative weight for each queue that determines the percentage of service time the switch services each queue before moving on to the next queue. This prevents the head-of-line blocking that can occur with strict priority queuing.

Command Attributes

- **WRR** – Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights 1, 4, 16, and 64 for queues 0 through 3 respectively. (This is the default selection.)
- **Strict** – Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues.

Web – Click Priority, Queue Mode. Select Strict or Wrr, then click Apply.



Queue Mode

Queue Mode: Wrr

CLI – The following sets the queue mode to strict priority service mode.

```
Console(config)#queue mode strict                                         4-149
Console(config)#exit
Console#show queue mode                                                   4-149

Queue mode: strict
Console#
```

Setting the Service Weight for Traffic Classes

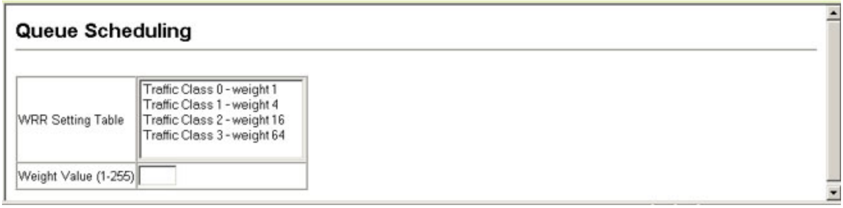
This switch uses the Weighted Round Robin (WRR) algorithm to determine the frequency at which it services each priority queue. As described in “Mapping CoS Values to Egress Queues” on page 3-97, the traffic classes are mapped to one of the four egress queues provided for each port. You can assign a weight to each of these queues (and thereby to the corresponding traffic priorities). This weight sets the frequency at which each queue will be polled for service, and subsequently affects the response time for software applications assigned a specific priority value.

Command Attributes

- **WRR Setting Table*** – Displays a list of weights for each traffic class (i.e., queue).
- **Weight Value** – Set a new weight for the selected traffic class. (Range: 1-255)

* CLI shows Queue ID.

Web – Click Priority, Queue Scheduling. Select the interface, highlight a traffic class (i.e., output queue), enter a weight, then click Apply.



Queue Scheduling

WRR Setting Table	Traffic Class 0 - weight 1 Traffic Class 1 - weight 4 Traffic Class 2 - weight 16 Traffic Class 3 - weight 64
Weight Value (1-255)	

CLI – The following example shows how to assign WRR weights to each of the priority queues.

```
Console(config)#queue bandwidth 2 8 16 128                                    4-147
Console(config)#exit
Console#show queue bandwidth                                                  4-149
 Queue ID  Weight
 --------  ------
    0        2
    1        8
    2        16
    3        128
Console#
```

Mapping Layer 3/4 Priorities to CoS Values

This switch supports several common methods of prioritizing layer 3/4 traffic to meet application requirements. Traffic priorities can be specified in the IP header of a frame, using the priority bits in the Type of Service (ToS) octet or the number of the TCP port. If priority bits are used, the ToS octet may contain three bits for IP Precedence or six bits for Differentiated Services Code Point (DSCP) service. When these services are enabled, the priorities are mapped to a Class of Service value by the switch, and the traffic then sent to the corresponding output queue.

Because different priority information may be contained in the traffic, this switch maps priority values to the output queues in the following manner:

- The precedence for priority mapping is IP Precedence or DSCP Priority, and then Default Port Priority.
- IP Precedence and DSCP Priority cannot both be enabled. Enabling one of these priority types will automatically disable the other.

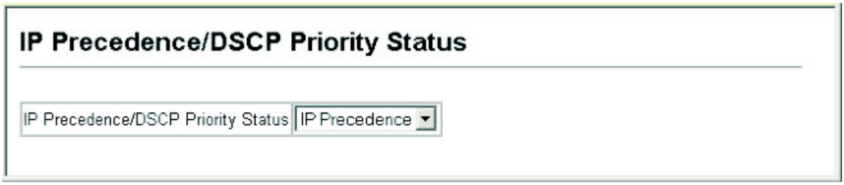
Selecting IP Precedence/DSCP Priority

The switch allows you to choose between using IP Precedence or DSCP priority. Select one of the methods or disable this feature.

Command Attributes

- **Disabled** – Disables both priority services. (This is the default setting.)
- **IP Precedence** – Maps layer 3/4 priorities using IP Precedence.
- **IP DSCP –** Maps layer 3/4 priorities using Differentiated Services Code Point Mapping.

Web – Click Priority, IP Precedence/DSCP Priority Status. Select Disabled, IP Precedence or IP DSCP from the scroll-down menu.



IP Precedence/DSCP Priority Status

IP Precedence/DSCP Priority Status: IP Precedence

CLI – The following example enables IP Precedence service on the switch.

```
Console(config)#map ip precedence                                 4-150
Console(config)#
```

Mapping IP Precedence

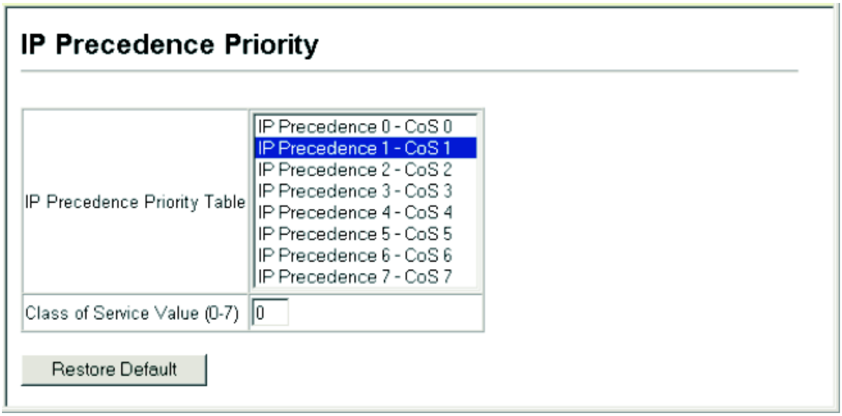
The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The default IP Precedence values are mapped one-to-one to Class of Service values (i.e., Precedence value 0 maps to CoS value 0, and so forth). Bits 6 and 7 are used for network control, and the other bits for various application types. ToS bits are defined in the following table.

Priority Level	Traffic Type	Priority Level	Traffic Type
7	Network Control	3	Flash
6	Internetwork Control	2	Immediate
5	Critical	1	Priority
4	Flash Override	0	Routine

Command Attributes

- **IP Precedence Priority Table –** Shows the IP Precedence to CoS map.
- **Class of Service Value –** Maps a CoS value to the selected IP Precedence value. Note that “0” represents low priority and “7” represent high priority.

Web – Click Priority, IP Precedence Priority. Select an entry from the IP Precedence Priority Table, enter a value in the Class of Service Value field, and then click Apply.



IP Precedence Priority

IP Precedence Priority Table

IP Precedence 0 - CoS 0
IP Precedence 1 - CoS 1
IP Precedence 2 - CoS 2
IP Precedence 3 - CoS 3
IP Precedence 4 - CoS 4
IP Precedence 5 - CoS 5
IP Precedence 6 - CoS 6
IP Precedence 7 - CoS 7

Class of Service Value (0-7) 0

CLI – The following example globally enables IP Precedence service on the switch, maps IP Precedence value 1 to CoS value 0 (on port 1), and then displays the IP Precedence settings.

```
Console(config)#map ip precedence                                    4-150
Console(config)#interface ethernet 1/1                               4-86
Console(config-if)#map ip precedence 1 cos 0                         4-151
Console(config-if)#end
Console#show map ip precedence ethernet 1/1                          4-154
Precedence mapping status: enabled

 Port      Precedence COS
 --------- ---------- ---
  Eth 1/ 1          0   0
  Eth 1/ 1          1   0
  Eth 1/ 1          2   2
  Eth 1/ 1          3   3
  Eth 1/ 1          4   4
  Eth 1/ 1          5   5
  Eth 1/ 1          6   6
  Eth 1/ 1          7   7
Console#
```

* Mapping specific values for IP Precedence is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

Mapping DSCP Priority

The DSCP is six bits wide, allowing coding for up to 64 different forwarding behaviors. The DSCP replaces the ToS bits, but it retains backward compatibility with the three precedence bits so that non-DSCP compliant, ToS-enabled devices, will not conflict with the DSCP mapping. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP default values are defined in the following table. Note that all the DSCP values that are not specified are mapped to CoS value 0.

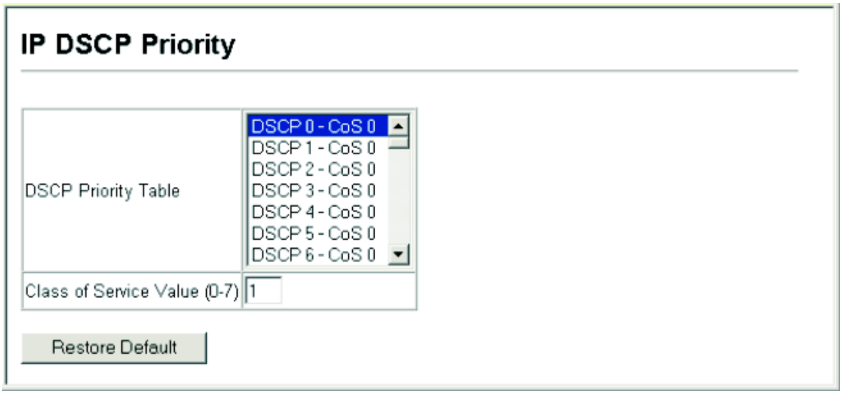
IP DSCP Value	CoS Value
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4
38, 40, 42	5
48	6
46, 56	7

Command Attributes

- **DSCP Priority Table –** Shows the DSCP Priority to CoS map.
- **Class of Service Value –** Maps a CoS value to the selected DSCP Priority value. Note that “0” represents low priority and “7” represent high priority.

Note: IP DSCP settings apply to all interfaces.

Web – Click Priority, IP DSCP Priority. Select an entry from the DSCP table, enter a value in the Class of Service Value field, then click Apply.



IP DSCP Priority

DSCP Priority Table	DSCP 0 - CoS 0 DSCP 1 - CoS 0 DSCP 2 - CoS 0 DSCP 3 - CoS 0 DSCP 4 - CoS 0 DSCP 5 - CoS 0 DSCP 6 - CoS 0
Class of Service Value (0-7)	1

CLI – The following example globally enables DSCP Priority service on the switch, maps DSCP value 0 to CoS value 1 (on port 1), and then displays the DSCP Priority settings.

```
Console(config)#map ip dscp                                           4-151
Console(config)#interface ethernet 1/1                                4-86
Console(config-if)#map ip dscp 1 cos 0                                4-152
Console(config-if)#end
Console#show map ip dscp ethernet 1/1                                 4-154
DSCP mapping status: enabled

 Port      DSCP COS
 --------- ---- ---
  Eth 1/ 1    0   0
  Eth 1/ 1    1   0
  Eth 1/ 1    2   0
  Eth 1/ 1    3   0
:
  Eth 1/ 1   61   0
  Eth 1/ 1   62   0
  Eth 1/ 1   63   0
Console#
```

* Mapping specific values for IP DSCP is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

Mapping IP Port Priority

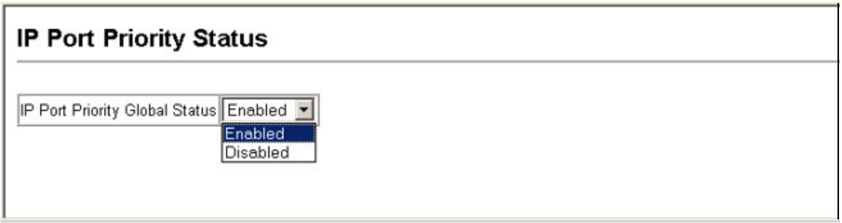
In the IP Port Priority page, for each switch port or trunk, you can map IP ports (TCP/UDP ports) to the switch's 4 traffic class queues.

Command Attributes

- **Current IP Port Table** – displays a list of IP ports with their mapped class of service queues.
- **IP Port** – to set a new IP port number.

Class of Service – to set a new class of service for an IP port. Note that "0" represents low priority and "3" represent high priority

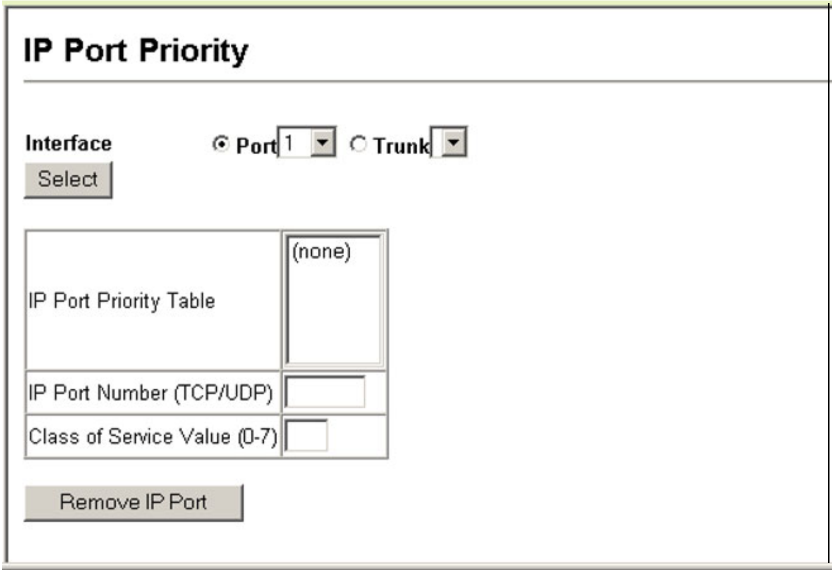
Web – Click Priority, IP Port Priority Status and then select Enabled.



IP Port Priority Status

IP Port Priority Global Status: Enabled

Click Priority, IP Port Priority. Select the port or trunk. To add an IP port, type the port number in the IP Port box and the new CoS value in the Class of Service box, then click Apply To delete an IP port setting, select the entry in the Current IP Port Table, then click Remove IP Port.



IP Port Priority

Interface ● Port 1 ○ Trunk

IP Port Priority Table	(none)
IP Port Number (TCP/UDP)	
Class of Service Value (0-7)	

CLI – The following example shows IP Port 80 mapped to CoS value 0 for ethernet port 1.

```
Console(config)#map ip port                                           4-153
Console(config)#interface ethernet 1/5
Console(config-if)#map ip port 80 cos 0                               4-153
Console(config-if)#end
Console# show map ip port ethernet 1/5                                4-155
TCP port mapping status: enabled

 Port      Port no. COS
 --------- -------- ---
  Eth 1/ 5       23   0
  Eth 1/ 5       80   0
  Eth 1/ 5     1020   6
Console#
```

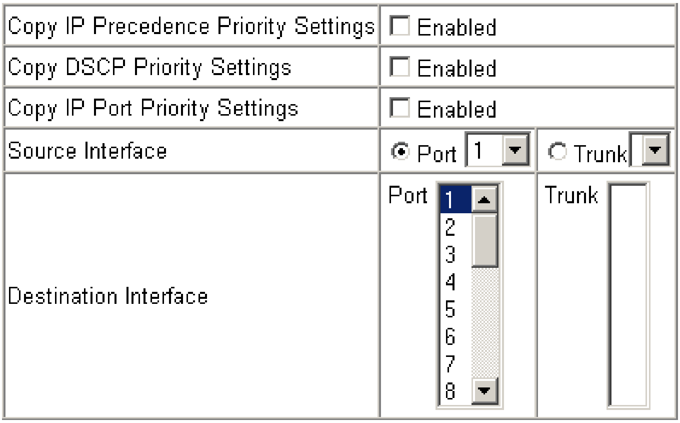
Copy Priority Settings

In the Copy Settings page you can copy the priority settings from a selected port or trunk to another selected port or trunk.

Command Attributes

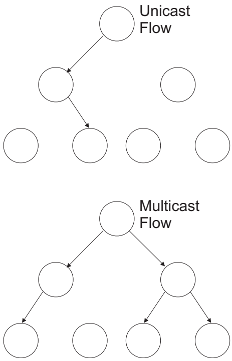
- **Source Interface** – The port or trunk from which the priority settings are copied.
- **Destination Interface** – The port or trunk to which the priority settings are copied.

Web – Click Priority, Copy Settings. Check the type of priority settings to be copied, select the source interface and destination interface, then click Copy Settings.



Copy IP Precedence Priority Settings	□ Enabled	
Copy DSCP Priority Settings	□ Enabled	
Copy IP Port Priority Settings	□ Enabled	
Source Interface	● Port 1	○ Trunk
Destination Interface	Port 1 2 3 4 5 6 7 8	Trunk

Multicast Filtering



Multicasting is used to support real-time applications such as videoconferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any hosts that want to receive the multicast register with their local multicast switch/router. Although this approach reduces the network overhead required by a multicast server, the broadcast traffic must be carefully pruned at every multicast switch/router it passes through to ensure that traffic is only passed on to the hosts which subscribed to this service.

This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts that want to receive a specific multicast service. It identifies the ports containing hosts requesting to join the service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service. This procedure is called multicast filtering.

The purpose of IP multicast filtering is to optimize a switched network's performance, so multicast packets will only be forwarded to those ports containing multicast group hosts or multicast routers/switches, instead of flooding traffic to all ports in the subnet (VLAN).

Layer 2 IGMP (Snooping and Query)

IGMP Snooping and Query – If multicast routing is not supported on other switches in your network, you can use IGMP Snooping and Query (page 3-107) to monitor IGMP service requests passing between multicast clients and servers, and dynamically configure the switch ports which need to forward multicast traffic.

Static IGMP Router Interface – If IGMP snooping cannot locate the IGMP querier, you can manually designate a known IGMP querier (i.e., a multicast router/switch) connected over the network to an interface on your switch (page 3-110). This interface will then join all the current multicast groups supported by the attached router/switch to ensure that multicast traffic is passed to all appropriate interfaces within the switch.

Static IGMP Host Interface – For multicast applications that you need to control more carefully, you can manually assign a multicast service to specific interfaces on the switch (page 3-112).

Configuring IGMP Snooping and Query Parameters

You can configure the switch to forward multicast traffic intelligently. Based on the IGMP query and report messages, the switch forwards traffic only to the ports that request multicast traffic. This prevents the switch from broadcasting the traffic to all ports and possibly disrupting network performance.

Command Usage

- IGMP Snooping – This switch can passively snoop on IGMP Query and Report packets transferred between IP multicast routers/switches and IP multicast host groups to identify the IP multicast group members. It simply monitors the IGMP packets passing through it, picks out the group registration information, and configures the multicast filters accordingly.
- IGMP Querier – A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected "querier" and assumes the role of querying the LAN for group members. It then propagates the service requests on to any upstream multicast switch/router to ensure that it will continue to receive the multicast service.

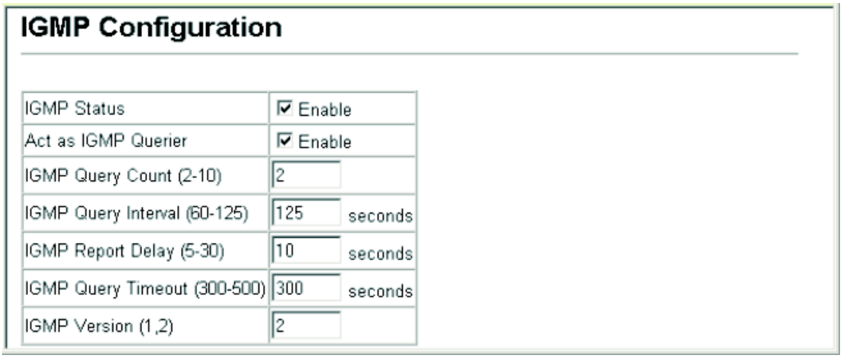
Note: Multicast routers use this information, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

Command Attributes

- **IGMP Status** – When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. This is also referred to as IGMP Snooping. (Default: Enabled)
- **Act as IGMP Querier** – When enabled, the switch can serve as the Querier, which is responsible for asking hosts if they want to receive multicast traffic. (Default: Enabled)
- **IGMP Query Count** – Sets the maximum number of queries issued for which there has been no response before the switch takes action to drop a client from the multicast group. (Range: 2-10, Default: 2)
- **IGMP Query Interval** – Sets the frequency at which the switch sends IGMP host-query messages. (Range: 60-125 seconds, Default: 125)
- **IGMP Report Delay** – Sets the time between receiving an IGMP Report for an IP multicast address on a port before the switch sends an IGMP Query out of that port and removes the entry from its list. (Range: 5-30 seconds, Default: 10)
- **IGMP Query Timeout** – The time the switch waits after the previous querier stops before it considers the router port (i.e., the interface which had been receiving query packets) to have expired.
(Range: 300-500 seconds, Default: 300)
- **IGMP Version** – Sets the protocol version for compatibility with other devices on the network. (Range: 1-2; Default: 2)

Notes: **1.** All systems on the subnet must support the same version.
2. Some attributes are only enabled for IGMPv2, including IGMP Report Delay and IGMP Query Timeout.

Web – Click IGMP Snooping, IGMP Configuration. Adjust the IGMP settings as required, and then click Apply. (The default settings are shown below.)



IGMP Configuration

IGMP Status	☑ Enable
Act as IGMP Querier	☑ Enable
IGMP Query Count (2-10)	2
IGMP Query Interval (60-125)	125 seconds
IGMP Report Delay (5-30)	10 seconds
IGMP Query Timeout (300-500)	300 seconds
IGMP Version (1,2)	2

CLI – This example modifies the settings for multicast filtering, and then displays the current status.

```
Console(config)#ip igmp snooping                                       4-156
Console(config)#ip igmp snooping querier                               4-160
Console(config)#ip igmp snooping query-count 10                        4-160
Console(config)#ip igmp snooping query-interval 100                    4-161
Console(config)#ip igmp snooping query-max-response-time 20            4-161
Console(config)#ip igmp snooping query-time-out 300                    4-162
Console(config)#ip igmp snooping version 2                             4-157
Console(config)#exit
Console#show ip igmp snooping                                          4-158
 Service status          : Enabled
 Querier status          : Enabled
 Query count             : 10
 Query interval          : 100 sec
 Query max response time : 20 sec
 Router port expire time: 300 sec
 IGMP snooping version   : Version 2
Console#
```

Displaying Interfaces Attached to a Multicast Router

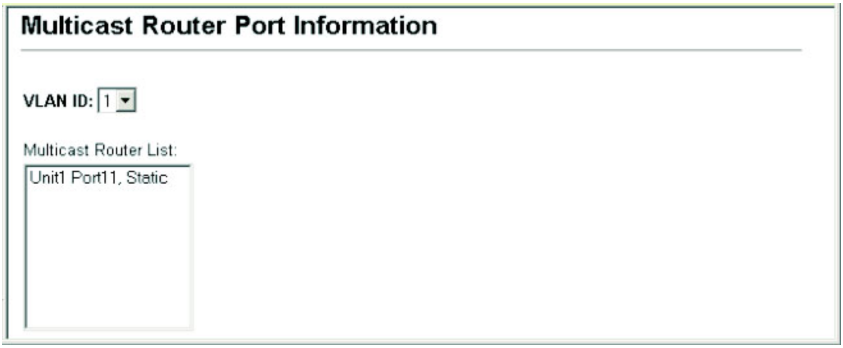
Multicast routers that are attached to ports on the switch use information obtained from IGMP, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet. These routers may be dynamically discovered by the switch or statically assigned to an interface on the switch.

You can use the Multicast Router Port Information page to display the ports on this switch attached to a neighboring multicast router/switch for each VLAN ID.

Command Attributes

- **VLAN ID** – ID of configured VLAN (1-4094).
- **Multicast Router List** – Multicast routers dynamically discovered by this switch or those that are statically assigned to an interface on this switch.

Web – Click IGMP Snooping, Multicast Router Port Information. Select the required VLAN ID from the scroll-down list to display the associated multicast routers.



Multicast Router Port Information

VLAN ID: 1

Multicast Router List:

Unit1 Port11, Static

CLI – This example shows that Port 11 has been statically configured as a port attached to a multicast router.

```
Console#show ip igmp snooping mrouter vlan 1                     4-163
 VLAN M'cast Router Port Type
 ---- ------------------ -------
    1           Eth 1/1  Static
```

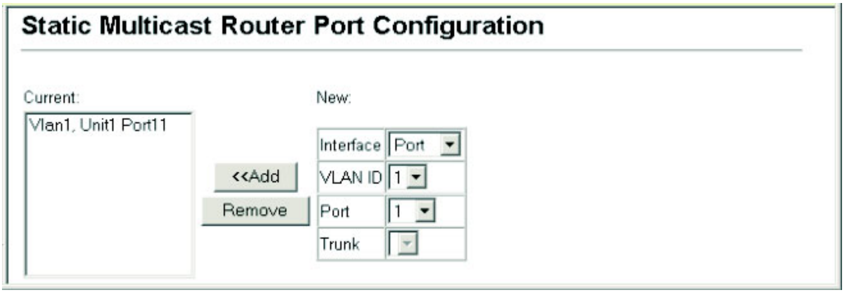
Specifying Static Interfaces for a Multicast Router

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/switch connected over the network to an interface (port or trunk) on your switch, you can manually configure the interface (and a specified VLAN) to join all the current multicast groups supported by the attached router. This can ensure that multicast traffic is passed to all the appropriate interfaces within the switch.

Command Attributes

- **Interface** – Activates the Port or Trunk scroll down list.
- **VLAN ID** – Selects the VLAN to propagate all multicast traffic coming from the attached multicast router.
- **Port or Trunk** – Specifies the interface attached to a multicast router.

Web – Click IGMP Snooping, Static Multicast Router Port Configuration. Specify the interfaces attached to a multicast router, indicate the VLAN which will forward all the corresponding multicast traffic, and then click Add. After you have finished adding interfaces to the list, click Apply.



Static Multicast Router Port Configuration

Current:
Vlan1, Unit1 Port11

New:

Interface	Port
VLAN ID	1
Port	1
Trunk	

CLI – This example configures port 11 as a multicast router port within VLAN 1.

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11     4-163
Console(config)#exit
Console#show ip igmp snooping mrouter vlan 1                     4-164
 VLAN M'cast Router Port Type
 ---- ------------------ -------
    1           Eth 1/1  Static
```

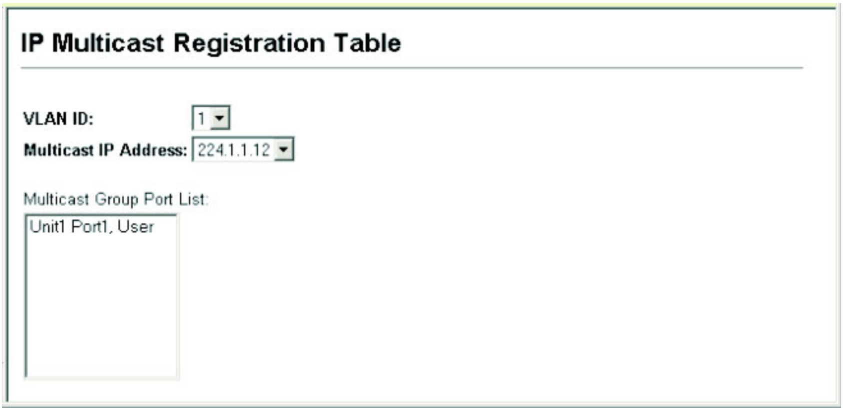
Displaying Port Members of Multicast Services

You can display the port members associated with a specified VLAN and multicast service.

Command Attribute

- **VLAN ID** – Selects the VLAN for which to display port members.
- **Multicast IP Address** – The IP address for a specific multicast service.
- **Multicast Group Port List** – Shows the interfaces that have already been assigned to the selected VLAN to propagate a specific multicast service.

Web – Click IGMP Snooping, IP Multicast Registration Table. Select a VLAN ID and the IP address for a multicast service from the scroll-down lists. The switch will display all the interfaces that are propagating this multicast service.



IP Multicast Registration Table

VLAN ID: 1

Multicast IP Address: 224.1.1.12

Multicast Group Port List:

Unit1 Port1, User

CLI – The following shows the multicast entries learned through IGMP snooping for VLAN 1:

```
Console#show mac-address-table multicast vlan 1 igmp-snooping        4-159
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1       224.1.2.3      Eth1/1    IGMP
Console#
```

Assigning Ports to Multicast Services

Multicast filtering can be dynamically configured using IGMP Snooping and IGMP Query messages as described in “Configuring IGMP Snooping and Query Parameters” on page 3-107. For certain applications that require tighter control, you may need to statically configure a multicast service on the switch. First add all the ports attached to participating hosts to a common VLAN, and then assign the multicast service to that VLAN group.

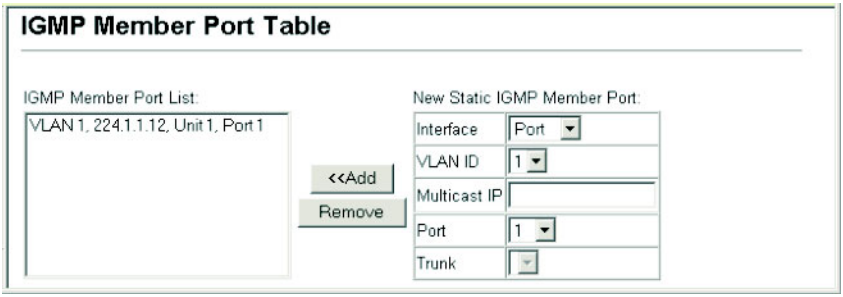
Command Usage

- Static multicast addresses are never aged out.
- When a multicast address is assigned to an interface in a specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.

Command Attribute

- **Interface** – Activates the Port or Trunk scroll down list.
- **VLAN ID** – Selects the VLAN to propagate all multicast traffic coming from the attached multicast router/switch.
- **Multicast IP** – The IP address for a specific multicast service
- **Port or Trunk** – Specifies the interface attached to a multicast router/switch.

Web – Click IGMP Snooping, IGMP Member Port Table. Specify the interface attached to a multicast service (via an IGMP-enabled switch or multicast router), indicate the VLAN that will propagate the multicast service, specify the multicast IP address, and click Add. After you have completed adding ports to the member list, click Apply.



IGMP Member Port Table

IGMP Member Port List:
VLAN 1, 224.1.1.12, Unit 1, Port 1

New Static IGMP Member Port:

Interface	Port
VLAN ID	1
Multicast IP	
Port	1
Trunk	

CLI – This example assigns a multicast address to VLAN 1, and then displays all the known multicast services supported on VLAN 1.

```
Console(config)#ip igmp snooping vlan 1 static 224.1.1.12 ethernet 1/12     4-157
Console(config)#exit
Console#show mac-address-table multicast vlan 1                             4-121
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1      224.1.1.12      Eth1/12    USER
    1       224.1.2.3      Eth1/12    IGMP
Console#
```

Chapter 4: Command Line Interface

This chapter describes how to use the Command Line Interface (CLI).

Using the Command Line Interface

Accessing the CLI

When accessing the management interface for the switch over a direct connection to the server’s console port, or via a Telnet connection, the switch can be managed by entering command keywords and parameters at the prompt. Using the switch's command-line interface (CLI) is very similar to entering commands on a UNIX system.

Console Connection

To access the switch through the console port, perform these steps:

1. At the console prompt, enter the user name and password. (The default user names are “admin” and “guest” with corresponding passwords of “admin” and “guest.”) When the administrator user name and password is entered, the CLI displays the “Console#” prompt and enters privileged access mode (i.e., Privileged Exec). But when the guest user name and password is entered, the CLI displays the “Console>” prompt and enters normal access mode (i.e., Normal Exec).
2. Enter the necessary commands to complete your desired tasks.
3. When finished, exit the session with the “quit” or “exit” command.

After connecting to the system through the console port, the login screen displays:

```
User Access Verification

Username: admin
Password:

      CLI session with the switch is opened.
      To end the CLI session, enter [Exit].

Console#
```

Telnet Connection

Telnet operates over the IP transport protocol. In this environment, your management station and any network device you want to manage over the network must have a valid IP address. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Each address consists of a network portion and host portion. For example, the IP address assigned to this switch, 10.1.0.1, consists of a network portion (10.1.0) and a host portion (1).

To access the switch through a Telnet session, you must first set the IP address for the switch, and set the default gateway if you are managing the switch from a different IP subnet. For example,

```
Console(config)#interface vlan 1
4-86
Console(config-if)#ip address 10.1.0.254 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254
```

If your corporate network is connected to another network outside your office or to the Internet, you need to apply for a registered IP address. However, if you are attached to an isolated network, then you can use any IP address that matches the network segment to which you are attached.

After you configure the switch with an IP address, you can open a Telnet session by performing these steps:

1. From the remote host, enter the Telnet command and the IP address of the device you want to access.
2. At the prompt, enter the user name and system password. The CLI will display the “Vty-0#” prompt for the administrator to show that you are using privileged access mode (i.e., Privileged Exec), or “Vty-0>” for the guest to show that you are using normal access mode (i.e., Normal Exec).
3. Enter the necessary commands to complete your desired tasks.
4. When finished, exit the session with the “quit” or “exit” command.

After entering the Telnet command, the login screen displays:

```
Username: admin
Password:

      CLI session with the switch is opened.
      To end the CLI session, enter [Exit].

Vty-0#
```

Note: You can open up to four sessions to the device via Telnet.

Entering Commands

This section describes how to enter CLI commands.

Keywords and Arguments

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters. For example, in the command “show interfaces status ethernet 1/5,” **show interfaces** and **status** are keywords, **ethernet** is an argument that specifies the interface type, and **1/5** specifies the unit/port.

You can enter commands as follows:

- To enter a simple command, enter the command keyword.
- To enter multiple commands, enter each command in the required order. For example, to enable Privileged Exec command mode, and display the startup configuration, enter:

  ```
  Console>enable
  Console#show startup-config
  ```
- To enter commands that require parameters, enter the required parameters after the command keyword. For example, to set a password for the administrator, enter:

  ```
  Console(config)#username admin password 0 smith
  ```

Minimum Abbreviation

The CLI will accept a minimum number of characters that uniquely identify a command. For example, the command “configure” can be entered as **con**. If an entry is ambiguous, the system will prompt for further input.

Command Completion

If you terminate input with a Tab key, the CLI will print the remaining characters of a partial keyword up to the point of ambiguity. In the “logging history” example, typing **log** followed by a tab will result in printing the command up to “**logging**.”

Getting Help on Commands

You can display a brief description of the help system by entering the **help** command. You can also display command syntax by using the “?” character to list keywords or parameters.

Showing Commands

If you enter a "?" at the command prompt, the system will display the first level of keywords for the current command class (Normal Exec or Privileged Exec) or configuration class (Global, ACL, Interface, Line, VLAN Database, or MSTP). You can also display a list of valid keywords for a specific command. For example, the command "**show ?**" displays a list of possible show commands:

```
onsole#show ?
  bridge-ext         Bridge extend information
  calendar           Date information
  controllers        Interface controller status
  dot1x              Show 802.1x content
  history            Information of history
  interfaces         Information of interfaces
  ip                 IP information
  line               TTY line information
  log                Show the records of login
  logging            Show the setting of login
  mac-address-table  Set configuration of the address table
  map                Map priority
  port               Characteristics of the port
  pvlan              Information of private VLAN
  queue              Information of priority queue
  radius-server      Radius server information
  running-config     The system configuration of running
  snmp               SNMP statistics
  spanning-tree      Specify spanning-tree
  ssh                Secure shell
  startup-config     The system configuration of starting up
  system             Information of system
  tacacs-server      Login by tacacs server
  users              Display information about terminal lines
  version            System hardware and software status
  vlan               Switch VLAN Virtual Interface
Console#show
```

The command "**show interfaces ?**" will display the following information:

```
Console#show interfaces ?
  counters       Information of interfaces counter
  status         Information of interfaces status
  switchport     Information of interfaces switchport
Console#
```

Partial Keyword Lookup

If you terminate a partial keyword with a question mark, alternatives that match the initial letters are provided. (Remember not to leave a space between the command and question mark.) For example "**s?**" shows all the keywords starting with "s."

```
Console#show s?
snmp           sntp           spanning-tree   ssh           startup-config
system
```

Negating the Effect of Commands

For many configuration commands you can enter the prefix keyword “**no**” to cancel the effect of a command or reset the configuration to the default value. For example, the **logging** command will log system messages to a host server. To disable logging, specify the **no logging** command. This guide describes the negation effect for all applicable commands.

Using Command History

The CLI maintains a history of commands that have been entered. You can scroll back through the history of commands by pressing the up arrow key. Any command displayed in the history list can be executed again, or first modified and then executed.

Using the **show history** command displays a longer list of recently executed commands.

Understanding Command Modes

The command set is divided into Exec and Configuration classes. Exec commands generally display information on system status or clear statistical counters. Configuration commands, on the other hand, modify interface parameters or enable certain switching functions. These classes are further divided into different modes. Available commands depend on the selected mode. You can always enter a question mark “**?**” at the prompt to display a list of the commands available for the current mode. The command classes and associated modes are displayed in the following table:

Class	Mode	
Exec	Normal Privileged	
Configuration	Global*	Interface Line VLAN Database

* You must be in Privileged Exec mode to access the Global configuration mode.
You must be in Global Configuration mode to access any of the other configuration modes.

Exec Commands

When you open a new console session on the switch with the user name and password “guest,” the system enters the Normal Exec command mode (or guest mode), displaying the “Console>” command prompt. Only a limited number of the commands are available in this mode. You can access all commands only from the Privileged Exec command mode (or administrator mode). To access Privilege Exec mode, open a new console session with the user name and password “admin.”

The system will now display the “Console#” command prompt. You can also enter Privileged Exec mode from within Normal Exec mode, by entering the **enable** command, followed by the privileged level password “super” (page 4-25).

To enter Privileged Exec mode, enter the following user names and passwords:

```
Username: admin
Password: [admin login password]

      CLI session with the switch is opened.
      To end the CLI session, enter [Exit].

Console#
```

```
Username: guest
Password: [guest login password]

      CLI session with the switch is opened.
      To end the CLI session, enter [Exit].

Console#enable
Password: [privileged level password]
Console#
```

Configuration Commands

Configuration commands are privileged level commands used to modify switch settings. These commands modify the running configuration only and are not saved when the switch is rebooted. To store the running configuration in non-volatile storage, use the **copy running-config startup-config** command.

The configuration commands are organized into different modes:

- Global Configuration - These commands modify the system level configuration, and include commands such as **hostname** and **snmp-server community**.
- Interface Configuration - These commands modify the port configuration such as **speed-duplex** and **negotiation**.
- Line Configuration - These commands modify the console port and Telnet configuration, and include command such as **parity** and **databits**.
- VLAN Configuration - Includes the command to create VLAN groups.

To enter the Global Configuration mode, enter the command **configure** in Privileged Exec mode. The system prompt will change to “Console(config)#” which gives you access privilege to all Global Configuration commands.

```
Console#configure
Console(config)#
```

To enter the other modes, at the configuration prompt type one of the following commands. Use the **exit** or **end** command to return to the Privileged Exec mode.

Mode	Command	Prompt	Page
Line	line {console | vty}	Console(config-line)#	4-9
Interface	interface {ethernet *port* | port-channel *id*| vlan *id*}	Console(config-if)#	4-91
VLAN	vlan database	Console(config-vlan)	4-135

For example, you can use the following commands to enter interface configuration mode, and then return to Privileged Exec mode

```
Console(config)#interface ethernet 1/5
.
.
.
Console(config-if)#exit
Console(config)#
```

Command Line Processing

Commands are not case sensitive. You can abbreviate commands and parameters as long as they contain enough letters to differentiate them from any other currently available commands or parameters. You can use the Tab key to complete partial commands, or enter a partial command followed by the “?” character to display a list of possible matches. You can also use the following editing keystrokes for command-line processing:

Keystroke	Function
Ctrl-A	Shifts cursor to start of command line.
Ctrl-B	Shifts cursor to the left one character.
Ctrl-C	Terminates the current task and displays the command prompt.
Ctrl-E	Shifts cursor to end of command line.
Ctrl-F	Shifts cursor to the right one character.
Ctrl-K	Deletes all characters from the cursor to the end of the line.
Ctrl-L	Repeats current command line on a new line.
Ctrl-N	Enters the next command line in the history buffer.
Ctrl-P	Enters the last command.
Ctrl-R	Repeats current command line on a new line.
Ctrl-U	Deletes from the cursor to the beginning of the line.
Ctrl-W	Deletes the last word typed.
Esc-B	Moves the cursor back one word.
Esc-D	Deletes from the cursor to the end of the word.
Esc-F	Moves the cursor forward one word.
Delete key or backspace key	Erases a mistake when entering a command.

Command Groups

The system commands can be broken down into the functional groups shown below.

Command Group	Description	Page
Line	Sets communication parameters for the serial port and Telnet, including baud rate and console time-out	4-9
General	Basic commands for entering privileged access mode, restarting the system, or quitting the CLI	4-18
System Management	Controls system logs, system passwords, user name, browser management options, and a variety of other system information	4-23
Flash/File	Manages code image or switch configuration files	4-57
Authentication	Configures logon access using local or remote authentication; also configures port security and IEEE 802.1x port access control	4-62
SNMP	Activates authentication failure traps; configures community access strings, and trap managers; also configures IP address filtering	4-78
DHCP	Configures DHCP client	4-84
Interface	Configures the connection parameters for all Ethernet ports, aggregated links, and VLANs	4-91
Mirror Port	Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port	4-97
Rate Limiting	Controls the maximum rate for traffic transmitted or received on a port	4-99
Link Aggregation	Statically groups multiple ports into a single logical trunk; configures Link Aggregation Control Protocol for port trunks	4-100
VDSL	Used to to configure and display communication parametersfor VDSL and ethernet ports on the switch and connected CPEs	4-103
Address Table	Configures the address table for filtering specified addresses, displays current entries, clears the table, or sets the aging time	4-120
Spanning Tree	Configures Spanning Tree settings for the switch	4-123
VLANs	Configures VLAN settings, and defines port membership for VLAN groups; also enables or configures private VLANs	4-135
Bridge Extension	Display default configuration settings for the Bridge Extension MIB and configure forbidden VLANs	4-144
Priority	Sets port priority for untagged frames, selects strict priority or weighted round robin, relative weight for each priority queue, also sets priority for TCP traffic types, IP precedence, and DSCP	4-145
Multicast Filtering	Configures IGMP multicast filtering, query parameters, and specifies ports attached to a multicast router	4-156
IP Interface	Configures IP address for the switch	4-164

The access mode shown in the following tables is indicated by these abbreviations:

NE (Normal Exec)
PE (Privileged Exec)
GC (Global Configuration)

LC (Line Configuration)
VC (VLAN Database Configuration)
IC (Interface Configuration)

Line Commands

You can access the onboard configuration program by attaching a VT100 compatible device to the server's serial port. These commands are used to set communication parameters for the serial port or Telnet (i.e., a virtual terminal).

Command	Function	Mode	Page
line	Identifies a specific line for configuration and starts the line configuration mode	GC	4-9
login	Enables password checking at login	LC	4-10
password	Specifies a password on a line	LC	4-11
exec-timeout	Sets the interval that the command interpreter waits until user input is detected	LC	4-12
password-thresh	Sets the password intrusion threshold, which limits the number of failed logon attempts	LC	4-12
silent-time*	Sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the **password-thresh** command	LC	4-13
databits*	Sets the number of data bits per character that are interpreted and generated by hardware	LC	4-14
parity*	Defines the generation of a parity bit	LC	4-14
speed*	Sets the terminal baud rate	LC	4-15
stopbits*	Sets the number of the stop bits transmitted per byte	LC	4-16
disconnect	Terminates a line connection	PE	4-16
show line	Displays a terminal line's parameters	NE, PE	4-17

* These commands only apply to the serial port.

line

This command identifies a specific line for configuration, and to process subsequent line configuration commands.

Syntax

line {**console** | **vty**}

- **console** - Console terminal line.
- **vty** - Virtual terminal for remote console access (i.e., Telnet).

Default Setting

There is no default line.

Command Mode

Global Configuration

Command Usage

Telnet is considered a virtual terminal connection and will be shown as “Vty” in screen displays such as show users. However, the serial communication parameters (e.g., databits) do not affect Telnet connections.

Example

To enter console line mode, enter the following command:

```
Console(config)#line console
Console(config-line)#
```

Related Commands

show line (4-17)
show users (4-55)

login

This command enables password checking at login. Use the **no** form to disable password checking and allow connections without a password.

Syntax

login [**local**]
no login

local - Selects local password checking. Authentication is based on the user name specified with the **username** command.

Default Setting

login local

Command Mode

Line Configuration

Command Usage

- There are three authentication modes provided by the switch itself at login:
- **login** selects authentication by a single global password as specified by the **password** line configuration command. When using this method, the management interface starts in Normal Exec (NE) mode.
- **login local** selects authentication via the user name and password specified by the **username** command (i.e., default setting). When using this method, the management interface starts in Normal Exec (NE) or Privileged Exec (PE) mode, depending on the user’s privilege level (0 or 15 respectively).

- **no login** selects no authentication. When using this method, the management interface starts in Normal Exec (NE) mode.
- This command controls login authentication via the switch itself. To configure user names and passwords for remote authentication servers, you must use the RADIUS or TACACS software installed on those servers.

Example

```
Console(config-line)#login local
Console(config-line)#
```

Related Commands

username (4-24)
password (4-11)

password

This command specifies the password for a line. Use the **no** form to remove the password.

Syntax

password {**0** | **7**} *password*
no password

- {**0** | **7**} - 0 means plain password, 7 means encrypted password
- *password* - Character string that specifies the line password. (Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default Setting

No password is specified.

Command Mode

Line Configuration

Command Usage

- When a connection is started on a line with password protection, the system prompts for the password. If you enter the correct password, the system shows a prompt. You can use the **password-thresh** command to set the number of times a user can enter an incorrect password before the system terminates the line connection and returns the terminal to the idle state.
- The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

```
Console(config-line)#password 0 secret
Console(config-line)#
```

Related Commands

login (4-10)
password-thresh (4-12)

exec-timeout

This command sets the interval that the system waits until user input is detected. Use the **no** form to restore the default.

Syntax

exec-timeout [*seconds*]
no exec-timeout

seconds - Integer that specifies the number of seconds.
(Range: 0 - 65535 seconds; 0: no timeout)

Default Setting

CLI: No timeout
Telnet: 10 minutes

Command Mode

Line Configuration

Command Usage

- If user input is detected within the timeout interval, the session is kept open; otherwise the session is terminated.
- This command applies to both the local console and Telnet connections.
- The timeout for Telnet cannot be disabled.

Example

To set the timeout to two minutes, enter this command:

```
Console(config-line)#exec-timeout 120
Console(config-line)#
```

password-thresh

This command sets the password intrusion threshold which limits the number of failed logon attempts. Use the **no** form to remove the threshold value.

Syntax

password-thresh *threshold*
no password-thresh

threshold - The number of allowed password attempts.
(Range: 1-120; 0: no threshold)

Default Setting

The default value is three attempts.

Command Mode

Line Configuration

Command Usage

- When the logon attempt threshold is reached, the system interface becomes silent for a specified amount of time before allowing the next logon attempt. (Use the **silent-time** command to set this interval.) When this threshold is reached for Telnet, the Telnet logon interface shuts down.
- This command applies to both the local console and Telnet connections.

Example

To set the password threshold to five attempts, enter this command:

```
Console(config-line)#password-thresh 5
Console(config-line)#
```

Related Commands

silent-time (4-13)

silent-time

This command sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the **password-thresh** command. Use the **no** form to remove the silent time value.

Syntax

silent-time [*seconds*]
no silent-time

seconds - The number of seconds to disable console response. (Range: 0-65535; 0: no silent-time)

Default Setting

The default value is no silent-time.

Command Mode

Line Configuration

Example

To set the silent time to 60 seconds, enter this command:

```
Console(config-line)#silent-time 60
Console(config-line)#
```

Related Commands

password-thresh (4-12)

databits

This command sets the number of data bits per character that are interpreted and generated by the console port. Use the **no** form to restore the default value.

Syntax

databits {**7** | **8**}
no databits

- 7 - Seven data bits per character.
- 8 - Eight data bits per character.

Default Setting

8 data bits per character

Command Mode

Line Configuration

Command Usage

The databits command can be used to mask the high bit on input from devices that generate 7 data bits with parity. If parity is being generated, specify 7 data bits per character. If no parity is required, specify 8 data bits per character.

Example

To specify 7 data bits, enter this command:

```
Console(config-line)#databits 7
Console(config-line)#
```

Related Commands

parity (4-14)

parity

This command defines the generation of a parity bit. Use the **no** form to restore the default setting.

Syntax

parity {**none** | **even** | **odd**}
no parity

- **none** - No parity
- **even** - Even parity
- **odd** - Odd parity

Default Setting

No parity

Command Mode

Line Configuration

Command Usage

Communication protocols provided by devices such as terminals and modems often require a specific parity bit setting.

Example

To specify no parity, enter this command:

```
Console(config-line)#parity none
Console(config-line)#
```

speed

This command sets the terminal line's baud rate. This command sets both the transmit (to terminal) and receive (from terminal) speeds. Use the **no** form to restore the default setting.

Syntax

speed *bps*
no speed

bps - Baud rate in bits per second.
(Options: 9600, 19200, 38400, 57600, 115200 bps, or auto)

Default Setting

auto

Command Mode

Line Configuration

Command Usage

Set the speed to match the baud rate of the device connected to the serial port. Some baud rates available on devices connected to the port might not be supported. The system indicates if the speed you selected is not supported. If you select the "auto" option, the switch will automatically detect the baud rate configured on the attached terminal, and adjust the speed accordingly.

Example

To specify 57600 bps, enter this command:

```
Console(config-line)#speed 57600
Console(config-line)#
```

stopbits

This command sets the number of the stop bits transmitted per byte. Use the **no** form to restore the default setting.

Syntax

stopbits {**1** | **2**}

- 1 - One stop bit
- 2 - Two stop bits

Default Setting

1 stop bit

Command Mode

Line Configuration

Example

To specify 2 stop bits, enter this command:

```
Console(config-line)#stopbits 2
Console(config-line)#
```

disconnect

Use this command to terminate an SSH, Telnet, or console connection.

Syntax

disconnect *session-id*

session-id – The session identifier for an SSH, Telnet or console connection. (Range: 0-4)

Command Mode

Privileged Exec

Command Usage

Specifying session identifier “0” will disconnect the console connection. Specifying any other identifiers for an active session will disconnect an SSH or Telnet connection.

Example

```
Console#disconnect 1
Console#
```

Related Commands

Event Logging Commands (4-35)
show users (4-55)

show line

This command displays the terminal line's parameters.

Syntax

show line [**console** | **vty**]

- **console** - Console terminal line.
- **vty** - Virtual terminal for remote console access (i.e., Telnet).

Default Setting

Shows all lines

Command Mode

Normal Exec, Privileged Exec

Example

To show all lines, enter this command:

```
Console#show line
 Console configuration:
  Password threshold: 3 times
  Interactive timeout: Disabled
  Silent time: Disabled
  Baudrate: 9600
  Databits: 8
  Parity: none
  Stopbits: 1
Vty configuration:
  Password threshold: 3 times
  Interactive timeout: 65535
```

General Commands

Command	Function	Mode	Page
enable	Activates privileged mode	NE	4-18
disable	Returns to normal mode from privileged mode	PE	4-19
configure	Activates global configuration mode	PE	4-19
show history	Shows the command history buffer	NE, PE	4-20
reload	Restarts the system	PE	4-21
end	Returns to Privileged Exec mode	any config. mode	4-21
exit	Returns to the previous configuration mode, or exits the CLI	any	4-21
quit	Exits a CLI session	NE, PE	4-22
help	Shows how to use help	any	NA
?	Shows options for command completion (context sensitive)	any	NA

enable

This command activates Privileged Exec mode. In privileged mode, additional commands are available, and certain commands display additional information. See “Understanding Command Modes” on page 4-5.

Syntax

enable *level*

level - Privilege level to log into the device.

The device has two predefined privilege levels: 0: Normal Exec, 15: Privileged Exec. Enter level 15 to access Privileged Exec mode.

Default Setting

Level 15

Command Mode

Normal Exec

Command Usage

- “super” is the default password required to change the command mode from Normal Exec to Privileged Exec. (To set this password, see the **enable password** command on page 4-25.)
- The “#” character is appended to the end of the prompt to indicate that the system is in privileged access mode.

Example

```
Console>enable
Password: [privileged level password]
Console#
```

Related Commands

disable (4-19)
enable password (4-25)

disable

This command returns to Normal Exec mode from privileged mode. In normal access mode, you can only display basic information on the switch's configuration or Ethernet statistics. To gain access to all commands, you must use the privileged mode. See “Understanding Command Modes” on page 4-5.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

The “>” character is appended to the end of the prompt to indicate that the system is in normal access mode.

Example

```
Console#disable
Console>
```

Related Commands

enable (4-18)

configure

This command activates Global Configuration mode. You must enter this mode to modify any settings on the switch. You must also enter Global Configuration mode prior to enabling some of the other configuration modes, including Interface Configuration, Line Configuration, VLAN Database Configuration, and Multiple Spanning Tree Configuration. See “Understanding Command Modes” on page 4-5.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#configure
Console(config)#
```

Related Commands

end (4-21)

show history

This command shows the contents of the command history buffer.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The history buffer size is fixed at 10 Execution commands and 10 Configuration commands.

Example

In this example, the show history command lists the contents of the command history buffer:

```
Console#show history
Execution command history:
 2 config
 1 show history

Configuration command history:
 4 interface vlan 1
 3 exit
 2 interface vlan 1
 1 end

Console#
```

The **!** command repeats commands from the Execution command history buffer when you are in Normal Exec or Privileged Exec Mode, and commands from the Configuration command history buffer when you are in any of the configuration modes. In this example, the **!2** command repeats the second command in the Execution history buffer (**config**).

```
Console#!2
Console#config
Console(config)#
```

reload

This command restarts the system.

Note: When the system is restarted, it will always run the Power-On Self-Test. It will also retain all configuration information stored in non-volatile memory by the **copy running-config startup-config** command.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

This command resets the entire system.

Example

This example shows how to reset the switch:

```
Console#reload
System will be restarted, continue <y/n>? y
```

end

This command returns to Privileged Exec mode.

Default Setting

None

Command Mode

Global Configuration, Interface Configuration, Line Configuration, VLAN Database Configuration, and Multiple Spanning Tree Configuration.

Example

This example shows how to return to the Privileged Exec mode from the Interface Configuration mode:

```
Console(config-if)#end
Console#
```

exit

This command returns to the previous configuration mode or exit the configuration program.

Default Setting

None

Command Mode

Any

Example

This example shows how to return to the Privileged Exec mode from the Global Configuration mode, and then quit the CLI session:

```
Console(config)#exit
Console#exit

Press ENTER to start session
User Access Verification

Username:
```

quit

This command exits the configuration program.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The quit and exit commands can both exit the configuration program.

Example

This example shows how to quit a CLI session:

```
Console#quit

Press ENTER to start session

User Access Verification

Username:
```

System Management Commands

These commands are used to control system logs, passwords, user names, browser configuration options, and display or configure a variety of other system information.

Command Group	Function	Page
Device Designation	Configures information that uniquely identifies this switch	4-23
User Access	Configures the basic user names and passwords for management access	4-24
IP Filter	Configures IP addresses that are allowed management access	4-26
Web Server	Enables management access via a Web browser	4-28
Secure Shell	Provides secure replacement for Telnet	4-31
Event Logging	Controls logging of error messages	4-35
SMTP Alerts	Configures SMTP email alerts	4-41
Time (System Clock)	Sets the system clock automatically via NTP/SNTP server or manually	4-45
System Status	Displays system configuration, active managers, and version information	4-50

Device Designation Commands

Command	Function	Mode	Page
prompt	Customizes the prompt used in PE and NE mode	GC	4-23
hostname	Specifies the host name for the switch	GC	4-24
snmp-server contact	Sets the system contact string	GC	4-79
snmp-server location	Sets the system location string	GC	4-79

prompt

This command customizes the CLI prompt. Use the **no** form to restore the default prompt.

Syntax

prompt *string*
no prompt

string - Any alphanumeric string to use for the CLI prompt. (Maximum length: 255 characters)

Default Setting

Console

Command Mode

Global Configuration

Example

```
Console(config)#prompt RD2
RD2(config)#
```

hostname

This command specifies or modifies the host name for this device. Use the **no** form to restore the default host name.

Syntax

hostname *name*

no hostname

name - The name of this host. (Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#hostname RD#1
Console(config)#
```

User Access Commands

The basic commands required for management access are listed in this section. This switch also includes other options for password checking via the console or a Telnet connection (page 4-9), user authentication via a remote authentication server (page 4-62), and host access authentication for specific ports (page 4-70).

Command	Function	Mode	Page
username	Establishes a user name-based authentication system at login	GC	4-24
enable password	Sets a password to control access to the Privileged Exec level	GC	4-25

username

This command adds named users, requires authentication at login, specifies or changes a user's password (or specify that no password is required), or specifies or changes a user's access level. Use the **no** form to remove a user name.

Syntax

username ***name*** {**access-level** *level* | **nopassword** |
password {**0** | **7**} ***password***}
no username *name*

- *name* - The name of the user.
  (Maximum length: 8 characters, case sensitive. Maximum users: 16)
- **access-level** *level* - Specifies the user level.
- The device has two predefined privilege levels:
  0: Normal Exec, **15**: Privileged Exec.
- **nopassword** - No password is required for this user to log in.

- {**0** | **7**} - 0 means plain password, 7 means encrypted password.
- **password** *password* - The authentication password for the user. (Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default Setting

- The default access level is Normal Exec.
- The factory defaults for the user names and passwords are:

username	access-level	password
guest	0	guest
admin	15	admin

Command Mode

Global Configuration

Command Usage

The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

This example shows how the set the access level and password for a user.

```
Console(config)#username bob access-level 15
Console(config)#username bob password 0 smith
Console(config)#
```

enable password

After initially logging onto the system, you should set the Privileged Exec password. Remember to record it in a safe place. This command controls access to the Privileged Exec level from the Normal Exec level. Use the **no** form to reset the default password.

Syntax

enable password [**level** *level*] {**0** | **7**} *password*
no enable password [**level** *level*]

- **level** *level* - Level 15 for Privileged Exec. (Levels 0-14 are not used.)
- {**0** | **7**} - 0 means plain password, 7 means encrypted password.
- *password* - password for this privilege level. (Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default Setting

- The default is level 15.
- The default password is “super”

Command Mode

Global Configuration

Command Usage

- You cannot set a null password. You will have to enter a password to change the command mode from Normal Exec to Privileged Exec with the **enable** command (page 4-18).
- The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

```
Console(config)#enable password level 15 0 admin
Console(config)#
```

Related Commands

enable (4-18)

IP Filter Commands

Command	Function	Mode	Page
management	Configures IP addresses that are allowed management access	GC	4-26
show management	Displays the switch to be monitored or configured from a browser	PE	4-27

management

This command specifies the client IP addresses that are allowed management access to the switch through various protocols. Use the **no** form to restore the default setting.

Syntax

[**no**] **management** {**all-client** | **http-client** | **snmp-client** | **telnet-client**}
start-address [*end-address*]

- **all-client** - Adds IP address(es) to the SNMP, Web and Telnet groups.
- http-client - Adds IP address(es) to the Web group.
- snmp-client - Adds IP address(es) to the SNMP group.
- **telnet-client** - Adds IP address(es) to the Telnet group.
- start-address - A single IP address, or the starting address of a range.
- end-address - The end address of a range.

Default Setting

All addresses

Command Mode

Global Configuration

Command Usage

- If anyone tries to access a management interface on the switch from an invalid address, the switch will reject the connection, enter an event message in the system log, and send a trap message to the trap manager.
- IP address can be configured for SNMP, Web and Telnet access respectively. Each of these groups can include up to five different sets of addresses, either individual addresses or address ranges.
- When entering addresses for the same group (i.e., SNMP, Web or Telnet), the switch will not accept overlapping address ranges. When entering addresses for different groups, the switch will accept overlapping address ranges.
- You cannot delete an individual address from a specified range. You must delete the entire range, and reenter the addresses.
- You can delete an address range just by specifying the start address, or by specifying both the start address and end address.

Example

This example restricts management access to the indicated addresses.

```
Console(config)#management all-client 192.168.1.19
Console(config)#management all-client 192.168.1.25 192.168.1.30
Console#
```

show management

This command displays the client IP addresses that are allowed management access to the switch through various protocols.

Syntax

show management {**all-client** | **http-client** | **snmp-client** | **telnet-client**}

- **all-client** - Adds IP address(es) to the SNMP, Web and Telnet groups.
- http-client - Adds IP address(es) to the Web group.
- snmp-client - Adds IP address(es) to the SNMP group.
- **telnet-client** - Adds IP address(es) to the Telnet group.

Command Mode

Global Configuration

Example

```
Console#show management all-client
Management Ip Filter
 Http-Client:
   Start ip address      End ip address
-----------------------------------------------
1. 192.168.1.19          192.168.1.19
2. 192.168.1.25          192.168.1.30

 Snmp-Client:
   Start ip address      End ip address
-----------------------------------------------
1. 192.168.1.19          192.168.1.19
2. 192.168.1.25          192.168.1.30

 Telnet-Client:
   Start ip address      End ip address
-----------------------------------------------
1. 192.168.1.19          192.168.1.19
2. 192.168.1.25          192.168.1.30

Console#
```

Web Server Commands

Command	Function	Mode	Page
ip http port	Specifies the port to be used by the Web browser interface	GC	4-28
ip http server	Allows the switch to be monitored or configured from a browser	GC	4-29
ip http secure-server	Enables HTTPS/SSL for encrypted communications	GC	4-29
ip http secure-port	Specifies the UDP port number for HTTPS/SSL	GC	4-30
ip telnet server	Enables Telnet acces to the switch	GC	4-31

ip http port

This command specifies the TCP port number used by the Web browser interface. Use the **no** form to use the default port.

Syntax

ip http port *port-number*
no ip http port

port-number - The TCP port to be used by the browser interface. (Range: 1-65535)

Default Setting

80

Command Mode

Global Configuration

Example

```
Console(config)#ip http port 769
Console(config)#
```

Related Commands

ip http server (4-29)

ip http server

This command allows this device to be monitored or configured from a browser. Use the **no** form to disable this function.

Syntax

[**no**] **ip http server**

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#ip http server
Console(config)#
```

Related Commands

ip http port (4-28)

ip http secure-server

This command enables the secure hypertext transfer protocol (HTTPS) over the Secure Socket Layer (SSL), providing secure access (i.e., an encrypted connection) to the switch’s Web interface. Use the **no** form to disable this function.

Syntax

[**no**] **ip http secure-server**

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

- Both HTTP and HTTPS service can be enabled independently on the switch. However, you cannot configure the HTTP and HTTPS servers to use the same UDP port.

- If you enable HTTPS, you must indicate this in the URL that you specify in your browser: **https**://*device*[:*port_number*]
- When you start HTTPS, the connection is established in this way:
- The client authenticates the server using the server’s digital certificate.
- The client and server negotiate a set of security protocols to use for the connection.
- The client and server generate session keys for encrypting and decrypting data.
- The client and server establish a secure encrypted connection.
- A padlock icon should appear in the status bar for Internet Explorer 5.x and Netscape Navigator 4.x or later versions.
- The following Web browsers and operating systems currently support HTTPS:

Web Browser	**Operating System**
Internet Explorer 5.0 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP
Netscape Navigator 4.76 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP, Solaris 2.6

- To specify a secure-site certificate, see “Replacing the Default Secure-site Certificate” on page 3-29. Also refer to the **copy** command on page 4-57.

Example

```
Console(config)#ip http secure-server
Console(config)#
```

Related Commands

ip http secure-port (4-30)
copy tftp https-certificate (4-57)

ip http secure-port

This command specifies the UDP port number used for HTTPS/SSL connection to the switch’s Web interface. Use the **no** form to restore the default port.

Syntax

ip http secure-port *port_number*
no ip http secure-port

port_number – The UDP port used for HTTPS/SSL. (Range: 1-65535)

Default Setting

443

Command Mode

Global Configuration

Command Usage

- You cannot configure the HTTP and HTTPS servers to use the same port.
- If you change the HTTPS port number, clients attempting to connect to the HTTPS server must specify the port number in the URL, in this format: **https://***device***:***port_number*

Example

```
Console(config)#ip http secure-port 1000
Console(config)#
```

Related Commands

ip http secure-server (4-29)

ip telnet server

You can access the onboard configuration program by attaching a VT10 compatible device to the server’s serial port.

Syntax

[**no**] **ip telnet server**

Command Mode

Global Configuration

Example

```
Console#config
Console(config)#ip telnet server
Console(config-line)#
```

Secure Shell Commands

The Berkley-standard includes remote access tools originally designed for Unix systems. Some of these tools have also been implemented for Microsoft Windows and other environments. These tools, including commands such as *rsh* (remote shell), and *rexec* (remote execute), are not secure from hostile attacks.

The Secure Shell (SSH) includes server/client applications intended as a secure replacement for the older Berkley remote access tools. SSH provides remote management access via encrypted paths between the switch and SSH-enabled management station clients. The commands described in this section show how to configure the SSH server. However, you also need to install a SSH client on the management station when using this protocol to configure the switch. When the client contacts the switch via the SSH protocol, the switch generates a public-key that the client uses along with a local user name and password for access authentication.

Note: The switch supports only SSH Version 1.5.

Command	Function	Mode	Page
ip ssh server	Enables the SSH server on the switch	GC	4-32
ip ssh timeout	Specifies the authentication timeout for the SSH server	GC	4-35
ip ssh authentication-retries	Specifies the number of retries allowed by a client	GC	4-33
disconnect ssh	Terminates an SSH connection	PE	4-34
show ip ssh	Displays the status of the SSH server and the configured values for authentication timeout and retries	PE	4-34
show ssh	Displays the status of current SSH sessions	PE	4-35
show users	Shows SSH users, including privilege level and public key type	PE	4-55

ip ssh server

Use this command to enable the Secure Shell (SSH) server on this switch. Use the **no** form to disable this service.

Syntax

[**no**] **ip ssh server**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The SSH server supports up to four client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.
- The SSH server uses DSA or RSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.
- You must generate the host key before enabling the SSH server.

Example

```
Console#ip ssh crypto host-key generate dsa
Console#configure
Console(config)#ip ssh server
Console(config)#
```

Related Commands

Event Logging Commands (4-35)

ip ssh timeout

Use this command to configure the timeout for the SSH server. Use the **no** form to restore the default setting.

Syntax

ip ssh timeout *seconds*
no ip ssh timeout

seconds – The timeout for client response during SSH negotiation. (Range: 1-120)

Default Setting

10 seconds

Command Mode

Global Configuration

Command Usage

The timeout specifies the interval the switch will wait for a response from the client during the SSH negotiation phase. Once an SSH session has been established, the timeout for user input is controlled by the exec-timeout command for vty sessions.

Example

```
Console(config)#ip ssh timeout 60
Console(config)#
```

Related Commands

exec-timeout (4-12)
show ip ssh (4-34)

ip ssh authentication-retries

Use this command to configure the number of times the SSH server attempts to reauthenticate a user. Use the **no** form to restore the default setting.

Syntax

ip ssh authentication-retries *count*
no ip ssh authentication-retries

count – The number of authentication attempts permitted after which the interface is reset. (Range: 1-5)

Default Setting

3

Command Mode

Global Configuration

Example

```
Console(config)#ip ssh authentication-retires 2
Console(config)#
```

Related Commands

show ip ssh (4-34)

disconnect ssh

Use this command to terminate a Secure Shell (SSH) client connection.

Syntax

disconnect ssh *connection-id*

connection-id – The session identifier as displayed in the **show ssh** command.

Command Mode

Privileged Exec

Example

```
Console#disconnect ssh 0
Console#
```

show ip ssh

Use this command to display the connection settings used when authenticating client access to the SSH server.

Command Mode

Privileged Exec

Example

```
Console#show ip ssh
Information of secure shell
SSH status: enable
SSH authentication timeout: 120
SSH authentication retries: 3
Console#
```

show ssh

Use this command to display the current SSH server connections.

Command Mode

Privileged Exec

Example

```
Console#show ssh
Information of secure shell
Session Username Version Encrypt method Negotiation state
------- -------- ------- ------------- -----------------
      0    admin   1.5      cipher-3des   session-started
Console#
```

Field	Description
Session	The session number. (Range: 0-3)
Username	The user name of the client.
Version	The Secure Shell version number.
Negotiation State	The authentication negotiation state. (Values: negotiation-started, authentication-started, session-started)
Encryption Method	The encryption method is automatically negotiated between the client and server. Options for SSHv1.5 include: des, 3des *Terminology:* des – Data Encryption Standard (56-bit key) 3des – Triple-DES (Uses three iterations of DES, 112-bit key)

Event Logging Commands

Command	Function	Mode	Page
logging on	Controls logging of error messages	GC	4-36
logging history	Limits syslog messages saved to switch memory based on severity	GC	4-37
logging host	Adds a syslog server host IP address that will receive logging messages	GC	4-38
logging facility	Sets the facility type for remote logging of syslog messages	GC	4-38
logging trap	Limits syslog messages saved to a remote server based on severity	GC	4-39
clear logging	Clears messages from the logging buffer	PE	4-39
show logging	Displays the state of logging	PE	4-40

logging on

This command controls logging of error messages, sending debug or error messages to switch memory. The **no** form disables the logging process.

Syntax

[**no**] **logging on**

Default Setting

None

Command Mode

Global Configuration

Command Usage

The logging process controls error messages saved to switch memory. You can use the logging history command to control the type of error messages that are stored.

Example

```
Console(config)#logging on
Console(config)#
```

Related Commands

logging history (4-37)
clear logging (4-39)

logging history

This command limits syslog messages saved to switch memory based on severity. The **no** form returns the logging of syslog messages to the default level.

Syntax

logging history {**flash** | **ram**} *level*
no logging history {**flash** | **ram**}

- **flash** - Event history stored in flash memory (i.e., permanent memory).
- **ram** - Event history stored in temporary RAM (i.e., memory flushed on power reset).
- *level* - One of the level arguments listed below. Messages sent include the selected level down to level 0. (Range: 0-7)

Level Argument	Level	Description
debugging	7	Debugging messages
informational	6	Informational messages only
notifications	5	Normal but significant condition, such as cold start
warnings	4	Warning conditions (e.g., return false, unexpected return)
errors	3	Error conditions (e.g., invalid input, default used)
critical	2	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)
alerts	1	Immediate action needed
emergencies	0	System unusable

* There are only Level 2, 5 and 6 error messages for the current firmware release.

Default Setting

Flash: errors (level 3 - 0)
RAM: warnings (level 7 - 0)

Command Mode

Global Configuration

Command Usage

The message level specified for flash memory must be a higher priority (i.e., numerically lower) than that specified for RAM.

Example

```
Console(config)#logging history ram 0
Console(config)#
```

logging host

This command adds a syslog server host IP address that will receive logging messages. Use the **no** form to remove a syslog server host.

Syntax

[**no**] **logging host** *host_ip_address*

host_ip_address - The IP address of a syslog server.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- By using this command more than once you can build up a list of host IP addresses.
- The maximum number of host IP addresses allowed is five.

Example

```
Console(config)#logging host 10.1.0.3
Console(config)#
```

logging facility

This command sets the facility type for remote logging of syslog messages. Use the **no** form to return the type to the default.

Syntax

[**no**] **logging facility** *type*

type - A number that indicates the facility used by the syslog server to dispatch log messages to an appropriate service. (Range: 16-23)

Default Setting

23

Command Mode

Global Configuration

Command Usage

The command specifies the facility type tag sent in syslog messages. (See RFC 3164.) This type has no effect on the kind of messages reported by the switch. However, it may be used by the syslog server to sort messages or to store messages in the corresponding database.

Example

```
Console(config)#logging facility 19
Console(config)#
```

logging trap

This command limits syslog messages saved to a remote server based on severity. Use the **no** form to return the remote logging of syslog messages to the default level.

Syntax

[**no**] **logging trap** *level*

level - One of the level arguments listed below. Messages sent include the selected level up through level 0. (Refer to the table on page 4-37.)

Default Setting

Level 3 - 0

Command Mode

Global Configuration

Example

```
Console(config)#logging trap 4
Console(config)#
```

clear logging

This command clears messages from the log buffer.

Syntax

clear logging [**flash** | **ram**]

- **flash** - Event history stored in flash memory (i.e., permanent memory).
- **ram** - Event history stored in temporary RAM (i.e., memory flushed on power reset).

Default Setting

Flash and RAM

Command Mode

Privileged Exec

Example

```
Console#clear logging
Console#
```

Related Commands

show logging (4-40)

show logging

This command displays the logging configuration, along with any system and event messages stored in memory.

Syntax

show logging {**flash** | **ram** | **sendmail** | **trap**}

- **flash** - Event history stored in flash memory (i.e., permanent memory).
- **ram** - Event history stored in temporary RAM (i.e., memory flushed on power reset).
- **sendmail** - Displays settings for the SMTP event handler (page 4-44).
- **trap** - Displays settings for the trap function.

Default Setting

None

Command Mode

Privileged Exec

Example

The following example shows that system logging is enabled, the message level for flash memory is “errors” (i.e., default level 3 - 0), the message level for RAM is “debugging” (i.e., default level 7 - 0), and lists one sample error

```
Console#show logging flash
Syslog logging: Enable
History logging in FLASH: level errors
[0] 0:0:5 1/1/1 "PRI_MGR_InitDefault function fails."
   level: 3, module: 13, function: 0, and event no.: 0
Console#show logging ram
Syslog logging: Enable
History logging in RAM: level debugging
[0] 0:0:5 1/1/1 PRI_MGR_InitDefault function fails."
   level: 3, module: 13, function: 0, and event no.: 0
Console#
```

Field	Description
Syslog logging	Shows if system logging has been enabled via the **logging on** command.
History logging in FLASH	The message level(s) reported based on the **logging history** command.
History logging in RAM	The message level(s) reported based on the **logging history** command.
Messages	Any system and event messages stored in memory.

The following example displays settings for the trap function.

```
Console#show logging trap
Syslog logging: Enable
REMOTELOG status: disable
REMOTELOG facility type: local use 7
REMOTELOG level type: Debugging messages
REMOTELOG server IP address: 1.2.3.4
REMOTELOG server IP address: 0.0.0.0
REMOTELOG server IP address: 0.0.0.0
REMOTELOG server IP address: 0.0.0.0
REMOTELOG server IP address: 0.0.0.0
Console#
```

Field	Description
Syslog logging	Shows if system logging has been enabled via the **logging on** command.
REMOTELOG status	Shows if remote logging has been enabled via the **logging trap** command.
REMOTELOG facility type	The facility type for remote logging of syslog messages as specified in the **logging facility** command.
REMOTELOG level type	The severity threshold for syslog messages sent to a remote server as specified in the **logging trap** command.
REMOTELOG server IP address	The address of syslog servers as specified in the **logging host** command.

Related Commands

show logging sendmail (4-44)

SMTP Alert Commands

Configures SMTP event handling, and forwarding of alert messages to the specified SMTP servers and email recipients.

Command	Function	Mode	Page
logging sendmail host	SMTP servers to receive alert messages	GC	4-42
logging sendmail level	Severity threshold used to trigger alert messages	GC	4-42
logging sendmail source-email	Email address used for “From” field of alert messages	GC	4-43
logging sendmail destination-email	Email recipients of alert messages	GC	4-43
logging sendmail	Enables SMTP event handling	GC	4-44
show logging sendmail	Displays SMTP event handler settings	NE, PE	4-44

logging sendmail host

This command specifies SMTP servers that will be sent alert messages. Use the **no** form to remove an SMTP server.

Syntax

[**no**] **logging sendmail host** *ip_address*

ip_address - IP address of an SMTP server that will be sent alert messages for event handling.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- You can specify up to three SMTP servers for event handing. However, you must enter a separate command to specify each server.
- To send email alerts, the switch first opens a connection, sends all the email alerts waiting in the queue one by one, and finally closes the connection.
- To open a connection, the switch first selects the server that successfully sent mail during the last connection, or the first server configured by this command. If it fails to send mail, the switch selects the next server in the list and tries to send mail again. If it still fails, the system will repeat the process at a periodic interval. (A trap will be triggered if the switch cannot successfully open a connection.)

Example

```
Console(config)#logging sendmail host 192.168.1.19
Console(config)#
```

logging sendmail level

This command sets the severity threshold used to trigger alert messages.

Syntax

logging sendmail level [*level*]

level - One of the system message levels (page 4-37). Messages sent include the selected level down to level 0. (Range: 0-7; Default: 7)

Default Setting

Level 7

Command Mode

Global Configuration

Command Usage

The specified level indicates an event threshold. All events at this level or higher will be sent to the configured email recipients. (For example, using Level 7 will report all events from level 7 to level 0.)

Example

This example will send email alerts for system errors from level 3 through 0.

```
Console(config)#logging sendmail level 3
Console(config)#
```

logging sendmail source-email

This command sets the email address used for the “From” field in alert messages.

Syntax

logging sendmail source-email *email-address*

email-address - The source email address used in alert messages. (Range: 1-41 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

You may use an symbolic email address that identifies the switch, or the address of an administrator responsible for the switch.

Example

This example will send email alerts for system errors from level 3 through 0.

```
Console(config)#logging sendmail source-email bill@this-company.com
Console(config)#
```

logging sendmail destination-email

This command specifies the email recipients of alert messages. Use the **no** form to remove a recipient.

Syntax

[**no**] **logging sendmail destination-email** *email-address*

email-address - The source email address used in alert messages. (Range: 1-41 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

You can specify up to five recipients for alert messages. However, you must enter a separate command to specify each recipient.

Example

```
Console(config)#logging sendmail destination-email ted@this-company.com
Console(config)#
```

logging sendmail

This command enables SMTP event handling. Use the **no** form to disable this function.

Syntax

[**no**] **logging sendmail**

Default Setting

Disabled

Command Mode

Global Configuration

Example

```
Console(config)#logging sendmail
Console(config)#
```

show logging sendmail

This command displays the settings for the SMTP event handler.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show logging sendmail
SMTP servers
-----------------------------------------------
192.168.1.19
SMTP minimum severity level: 7

SMTP destination email addresses
-----------------------------------------------
ted@this-company.com

SMTP source email address: bill@this-company.com

SMTP status: Enable

Console#
```

Time Commands

The system clock can be dynamically set by polling a set of specified time servers (NTP or SNTP), or by using information broadcast by local time servers.

Command	Function	Mode	Page
sntp client	Accepts time from specified time servers	GC	4-45
sntp server	Specifies one or more time servers	GC	4-46
sntp poll	Sets the interval at which the client polls for time	GC	4-47
sntp broadcast client	Accepts time from any time broadcast server	GC	4-48
show sntp	Shows current SNTP configuration settings	NE, PE	4-48
clock timezone	Sets the time zone for the switch’s internal clock	GC	4-49
calendar set	Sets the system date and time	PE	4-49
show calendar	Displays the current date and time setting	NE, PE	4-50

sntp client

This command enables SNTP client requests for time synchronization from NTP or SNTP time servers specified with the **sntp servers** command. Use the **no** form to disable SNTP client requests.

Syntax

[**no**] **sntp client**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The time acquired from time servers is used to record accurate dates and times for log events. Without SNTP, the switch only records the time starting from the factory default set at the last bootup (i.e., 00:00:00, Jan. 1, 2001).
- This command enables client time requests to time servers specified via the **sntp servers** command. It issues time synchronization requests based on the interval set via the **sntp poll** command.
- The SNTP time query method is set to client mode when the first **sntp client** command is issued. However, if the **sntp broadcast client** command is issued, then the **no sntp broadcast client** command must be used to return the switch to SNTP client mode.

Example

```
Console(config)#sntp server 10.1.0.19
Console(config)#sntp poll 60
Console(config)#sntp client
Console(config)#end
Console#show sntp
Current time:  Dec 23 02:52:44 2002
Poll interval: 60
Current mode: unicast
Console#
```

Related Commands

sntp server (4-46)
sntp poll (4-47)
sntp broadcast client (4-48)
show sntp (4-48)

sntp server

This command sets the IP address of the servers to which SNTP time requests are issued. Use the this command with no arguments to clear all time servers from the current list.

Syntax

sntp server [*ip1* [*ip2* [*ip3*]]]

ip - IP address of an time server (NTP or SNTP).
(Range: 1 - 3 addresses)

Default Setting

None

Command Mode

Global Configuration

Command Usage

This command specifies time servers from which the switch will poll for time updates when set to SNTP client mode. The client will poll the time servers in the order specified until a response is received. It issues time synchronization requests based on the interval set via the sntp poll command.

Example

```
Console(config)#sntp server 10.1.0.19
Console#
```

Related Commands

sntp client (4-45)
sntp poll (4-47)
show sntp (4-48)

sntp poll

This command sets the interval between sending time requests when the switch is set to SNTP client mode. Use the **no** form to restore to the default.

Syntax

sntp poll *seconds*
no sntp poll

seconds - Interval between time requests. (Range: 16-16384 seconds)

Default Setting

16 seconds

Command Mode

Global Configuration

Command Usage

This command is only applicable when the switch is set to SNTP client mode.

Example

```
Console(config)#sntp poll 60
Console#
```

Related Commands

sntp client (4-45)

sntp broadcast client

This command synchronizes the switch’s clock based on time broadcast from time servers (using the multicast address 224.0.1.1). Use the **no** form to disable SNTP broadcast client mode.

Syntax

[**no**] **sntp broadcast client**

Default Setting

Disabled

Command Mode

Global Configuration

Example

```
Console(config)#sntp broadcast client
Console#
```

show sntp

This command displays the current time and configuration settings for the SNTP client, and indicates whether or not the local time has been properly updated.

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command displays the current time, the poll interval used for sending time synchronization requests (when the switch is set to SNTP client mode), and the current SNTP mode (i.e., client or broadcast).

Example

```
Console#show sntp
Current time:  Dec 23 05:13:28 2002
Poll interval: 16
Current mode:  unicast
Console#
```

clock timezone

This command sets the time zone for the switch's internal clock.

Syntax

clock timezone *name* **hour** *hours* **minute** *minutes* {**before-utc** | **after-utc**}

- *name* - Name of time zone, usually an acronym. (Range: 1-29 characters)
- *hours* - Number of hours before/after UTC. (Range: 1-12 hours)
- *minutes* - Number of minutes before/after UTC. (Range: 0-59 minutes)
- **before-utc** - Sets the local time zone before (east) of UTC.
- **after-utc** - Sets the local time zone after (west) of UTC.

Default Setting

None

Command Mode

Global Configuration

Command Usage

This command sets the local time zone relative to the Coordinated Universal Time (UTC, formerly Greenwich Mean Time or GMT), based on the earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is east (before) or west (after) of UTC.

Example

```
Console(config)#clock timezone Japan hours 8 minute 0 after-UTC
Console(config)#
```

Related Commands

show sntp (4-48)

calendar set

This command sets the system clock.

Syntax

calendar set *hour min sec* {*day month year* | *month day year*}

- *hour* - Hour in 24-hour format. (Range: 0 - 23)
- *min* - Minute. (Range: 0 - 59)
- *sec* - Second. (Range: 0 - 59)
- *day* - Day of month. (Range: 1 - 31)
- *month* - **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december**
- *year* - Year (4-digit). (Range: 2001 - 2101)

Default Setting

None

Command Mode

Privileged Exec

Example

This example shows how to set the system clock to 15:12:34, February 1st, 2002.

```
Console#calendar set 15:12:34 1 February 2002
Console#
```

show calendar

This command displays the system clock.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show calendar set
 15:12:34 February 1 2002
Console#
```

System Status Commands

Command	Function	Mode	Page
show startup-config	Displays the contents of the configuration file (stored in flash memory) that is used to start up the system	PE	4-50
show running-config	Displays the configuration data currently in use	PE	4-53
show system	Displays system information	NE, PE	4-55
show users	Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet clients	NE, PE	4-55
show version	Displays version information for the system	NE, PE	4-56

show startup-config

This command displays the configuration file stored in non-volatile memory that is used to start up the system.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- Use this command in conjunction with the **show running-config** command to compare the information in running memory to the information stored in non-volatile memory.
- This command displays settings for key command modes. Each mode group is separated by “!” symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:
- SNMP community strings
- Users (names and access levels)
- VLAN database (VLAN ID, name and state)
- VLAN configuration settings for each interface
- Multiple spanning tree instances (name and interfaces)
- IP address configured for VLANs
- Routing protocol configuration settings
- Spanning tree settings
- Any configured settings for the console port and Telnet

Example

```
Console#show startup-config
building startup-config, please wait.....
!
!
username admin access-level 15
username admin password 0 admin
!
username guest access-level 0
username guest password 0 guest
!
enable password level 15 0 super
!
snmp-server community public ro
snmp-server community private rw
!
vlan database
 vlan 1 name DefaultVlan media ethernet state active
!
spanning-tree mst-configuration
!
interface ethernet 1/1
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
 lacp partner admin-key 0
 spanning-tree edge-port
.
.
.
interface vlan 1
 ip address dhcp
!
line console
!
line vty
!
end

Console#
```

Related Commands

show running-config (4-53)

show running-config

This command displays the configuration information currently in use.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- Use this command in conjunction with the **show startup-config** command to compare the information in running memory to the information stored in non-volatile memory.
- This command displays settings for key command modes. Each mode group is separated by "!" symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:
- SNMP community strings
- Users (names, access levels, and encrypted passwords)
- VLAN database (VLAN ID, name and state)
- VLAN configuration settings for each interface
- Multiple spanning tree instances (name and interfaces)
- IP address configured for VLANs
- Spanning tree settings
- Any configured settings for the console port and Telnet

Example

```
Console#show running-config
building running-config, please wait.....
!
!
snmp-server community private rw
snmp-server community public ro
!
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
vlan database
 vlan 1 name DefaultVlan media ethernet state active
!
!
interface ethernet 1/1
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
 queue cos-map 0 0 1 2
 queue cos-map 1 3 4
 queue cos-map 2 5 7
 efm pbo
.
.
.
!
interface vlan 1
 ip address 192.168.1.33 255.255.255.0
!
!
!
spanning-tree mode rstp
!
ip igmp snooping version 1
!
!
!
no map ip precedence
no map ip dscp
queue bandwidth 1 3 5 7
!
!
!
!
line console
!
line vty
!
end
Console#
```

Related Commands

show startup-config (4-50)

show system

This command displays system information.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

- For a description of the items shown by this command, refer to “Displaying System Information” on page 3-7.
- The POST results should all display “PASS.” If any POST test indicates “FAIL,” contact your distributor for assistance.

Example

```
Console#show system
System description: 20 10/100/1000 ports + 4 Gigabit Combo ports L2/L4
  managed standalone switch
System OID string: 1.3.6.1.4.1.259.6.10.51
System information
 System Up time: 0 days, 1 hours, 23 minutes, and 44.61 seconds
 System Name             : [NONE]
 System Location         : [NONE]
 System Contact          : [NONE]
 MAC address             : 00-30-f1-47-58-3a
 Web server              : enable
 Web server port         : 80
 Web secure server       : enable
 Web secure server port  : 443
 POST result
UART LOOP BACK Test..........PASS
DRAM Test....................PASS
Timer Test...................PASS
PCI Device 1 Test............PASS
PCI Device 2 Test............PASS
Switch Int Loopback test.....PASS

Done All Pass.
Console#
```

show users

Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet client.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The session used to execute this command is indicated by a "*" symbol next to the Line (i.e., session) index number.

Example

```
Console#show users
 Username accounts:
  Username Privilege Public-Key
  -------- --------- ----------
     admin        15       None
     guest         0       None

 Online users:
  Line        Username Idle time (h:m:s) Remote IP addr.
  ----------- -------- ----------------- ---------------
* 0   console    admin           0:00:00
  1     vty 0    admin           0:04:37      10.1.0.19

Console#
```

show version

This command displays hardware and software version information for the system.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

See "Displaying Switch Hardware/Software Versions" on page 3-9 for detailed information on the items displayed by this command.

Example

```
Console#show version
Unit1
 Serial number          :1111111111
 Hardware version       :R0A
 Number of ports        :24
 Main power status      :up
 Redundant power status :not present
Agent(master)
 Unit id                :1
 Loader version         :2.0.2.2
 Boot rom version       :2.0.2.3
 Operation code version :1.0.0.0
Console#
```

Flash/File Commands

These commands are used to manage the system code or configuration files.

Command	Function	Mode	Page
copy	Copies a code image or a switch configuration to or from flash memory or a TFTP server	PE	4-57
delete	Deletes a file or code image	PE	4-59
dir	Displays a list of files in flash memory	PE	4-60
whichboot	Displays the files booted	PE	4-61
boot system	Specifies the file or image used to start up the system	GC	4-61

copy

This command moves (upload/download) a code image or configuration file between the switch’s flash memory and a TFTP server. When you save the system code or configuration settings to a file on a TFTP server, that file can later be downloaded to the switch to restore system operation. The success of the file transfer depends on the accessibility of the TFTP server and the quality of the network connection.

Syntax

copy file {**file** | **running-config** | **startup-config** | **tftp**}
copy running-config {**file** | **startup-config** | **tftp**}
copy startup-config {**file** | **running-config** | **tftp**}
copy tftp {**file** | **running-config** | **startup-config** | **https-certificate**}

- **file** - Keyword that allows you to copy to/from a file.
- **running-config** - Keyword that allows you to copy to/from the current running configuration.
- **startup-config** - The configuration used for system initialization.
- **tftp** - Keyword that allows you to copy to/from a TFTP server.
- **https-certificate** - Copies an HTTPS certificate from an TFTP server to the switch.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- The system prompts for data required to complete the copy command.
- The destination file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”)
- Due to the size limit of the flash memory, the switch supports only two operation code files.
- The maximum number of user-defined configuration files depends on available memory.
- You can use “Factory_Default_Config.cfg” as the source to copy from the factory default configuration file, but you cannot use it as the destination.
- To replace the startup configuration, you must use **startup-config** as the destination.
- The Boot ROM and Loader cannot be uploaded or downloaded from the TFTP server. You must use a direct console connection and access the download menu during a boot up to download the Boot ROM (or diagnostic) image.

Example

The following example shows how to upload the configuration settings to a file on the TFTP server:

```
Console#copy file tftp
Choose file type:
 1. config:  2. opcode: <1-2>: 1
Source file name: startup
TFTP server ip address: 10.1.0.99
Destination file name: startup.01
TFTP completed.
Success.

Console#
```

The following example shows how to copy the running configuration to a startup file.

```
Console#copy running-config file
destination file name: startup
Write to FLASH Programming.
\Write to FLASH finish.
Success.

Console#
```

The following example shows how to download a configuration file:

```
Console#copy tftp startup-config
TFTP server ip address: 10.1.0.99
Source configuration file name: startup.01
Startup configuration file name [startup]:
Write to FLASH Programming.

\Write to FLASH finish.
Success.

Console#
```

This example shows how to copy a secure-site certificate from an TFTP server. It then reboots the switch to activate the certificate:

```
Console#copy tftp https-certificate
TFTP server ip address: 10.1.0.19
Source certificate file name: SS-certificate
Source private file name: SS-private
Private password: ********

Success.
Console#reload
System will be restarted, continue <y/n>? y
```

delete

This command deletes a file or image.

Syntax

delete *filename*

filename - Name of the configuration file or image name.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- If the file type is used for system startup, then this file cannot be deleted.
- “Factory_Default_Config.cfg” cannot be deleted.

Example

This example shows how to delete the test2.cfg configuration file from flash memory.

```
Console#delete test2.cfg
Console#
```

Related Commands

dir (4-60)

dir

This command displays a list of files in flash memory.

Syntax

dir [**boot-rom** | **config | opcode** [:*filename*]]

The type of file or image to display includes:

- **boot-rom** - Boot ROM (or diagnostic) image file.
- **config** - Switch configuration file.
- **opcode** - Run-time operation code image file.
- *filename* - Name of the file or image. If this file exists but contains errors, information on this file cannot be shown.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- If you enter the command **dir** without any parameters, the system displays all files.
- File information is shown below:

Column Heading	Description
file name	The name of the file.
file type	File types: Boot-Rom, Operation Code, and Config file.
startup	Shows if this file is used when the system is started.
size	The length of the file in bytes.

Example

The following example shows how to display all file information:

```
Console#dir
                       file name      file type startup size (byte)
-------------------------------- -------------- ------- -----------
                       diag_0060 Boot-Rom image       Y      111360
                       run_01642 Operation Code       N     1074304
                        run_0200 Operation Code       Y     1083008
      Factory_Default_Config.cfg    Config File       N        2574
                         startup    Config File       Y        2710
-------------------------------------------------------------------
                                        Total free space:         0
Console#
```

whichboot

This command displays which files were booted when the system powered up.

Default Setting

None

Command Mode

Privileged Exec

Example

This example shows the information displayed by the **whichboot** command. See the table under the **dir** command for a description of the file information displayed by this command.

```
Console#whichboot
        file name      file type startup size (byte)
----------------- -------------- ------- -----------
        diag_0060 Boot-Rom image       Y      111360
         run_0200 Operation Code       Y     1083008
          startup    Config File       Y        2710
Console#
```

boot system

This command specifies the image used to start up the system.

Syntax

boot system {**boot-rom**| **config** | **opcode**}: *filename*

The type of file or image to set as a default includes:

- **boot-rom** - Boot ROM.
- **config** - Configuration file.
- **opcode** - Run-time operation code.

The colon (:) is required.

filename - Name of the configuration file or image name.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- A colon (:) is required after the specified file type.
- If the file contains an error, it cannot be set as the default file.

Example

```
Console(config)#boot system config: startup
Console(config)#
```

Related Commands

dir (4-60)
whichboot (4-61)

Authentication Commands

You can configure this switch to authenticate users logging into the system for management access using local or RADIUS authentication methods. You can also enable port-based authentication for network client access using IEEE 802.1x.

Command Group	Function	Page
Authentication Sequence	Defines logon authentication method and precedence	4-62
RADIUS Client	Configures settings for authentication via a RADIUS server	4-63
TACACS+ Client	Configures settings for authentication via a TACACS+ server	4-67
Port Security	Configures secure addresses for a port	4-69
Port Authentication	Configures host authentication on specific ports using 802.1x	4-70

Authentication Sequence

Command	Function	Mode	Page
authentication login	Defines logon authentication method and precedence	GC	4-62

authentication login

This command defines the login authentication method and precedence. Use the **no** form to restore the default.

Syntax

authentication login {[**local**] [**radius**] [**tacacs**]}

- no authentication login
- **local** - Use local password.
- **radius** - Use RADIUS server password.
- **tacacs** - Use TACACS server password.

Default Setting

Local

Command Mode

Global Configuration

Command Usage

- RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.
- RADIUS and TACACS+ logon authentication assigns a specific privilege level for each user name and password pair. The user name, password, and privilege level must be configured on the authentication server.
- You can specify three authentication methods in a single command to indicate the authentication sequence. For example, if you enter "**authentication login radius tacacs local**," the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted on the TACACS+ server. If the TACACS+ server is not available, the local user name and password is checked.

Example

```
Console(config)#authentication login radius
Console(config)#
```

Related Commands

username - for setting the local user names and passwords (4-24)

RADIUS Client

Remote Authentication Dial-in User Service (RADIUS) is a logon authentication protocol that uses software running on a central server to control access to RADIUS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user or group that require management access to a switch.

Command	Function	Mode	Page
radius-server host	Specifies the RADIUS server	GC	4-64
radius-server port	Sets the RADIUS server network port	GC	4-64
radius-server key	Sets the RADIUS encryption key	GC	4-65
radius-server retransmit	Sets the number of retries	GC	4-65
radius-server timeout	Sets the interval between sending authentication requests	GC	4-66
show radius-server	Shows the current RADIUS settings	PE	4-66

radius-server host

This command specifies the RADIUS server. Use the **no** form to restore the default.

Syntax

radius-server host *host_ip_address*
no radius-server host

host_ip_address - IP address of server.

Default Setting

10.1.0.1

Command Mode

Global Configuration

Example

```
Console(config)#radius-server host 192.168.1.25
Console(config)#
```

radius-server port

This command sets the RADIUS server network port. Use the **no** form to restore the default.

Syntax

radius-server port *port_number*
no radius-server port

port_number - RADIUS server UDP port used for authentication messages. (Range: 1-65535)

Default Setting

1812

Command Mode

Global Configuration

Example

```
Console(config)#radius-server port 181
Console(config)#
```

radius-server key

This command sets the RADIUS encryption key. Use the **no** form to restore the default.

Syntax

radius-server key *key_string*
no radius-server key

key_string - Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 20 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#radius-server key green
Console(config)#
```

radius-server retransmit

This command sets the number of retries. Use the **no** form to restore the default.

Syntax

radius-server retransmit *number_of_retries*
no radius-server retransmit

number_of_retries - Number of times the switch will try to authenticate logon access via the RADIUS server. (Range: 1 - 30)

Default Setting

2

Command Mode

Global Configuration

Example

```
Console(config)#radius-server retransmit 5
Console(config)#
```

radius-server timeout

This command sets the interval between transmitting authentication requests to the RADIUS server. Use the **no** form to restore the default.

Syntax

radius-server timeout *number_of_seconds*
no radius-server timeout

number_of_seconds - Number of seconds the switch waits for a reply before resending a request. (Range: 1-65535)

Default Setting

5

Command Mode

Global Configuration

Example

```
Console(config)#radius-server timeout 10
Console(config)#
```

show radius-server

This command displays the current settings for the RADIUS server.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show radius-server
Server IP address: 10.1.0.1
 Communication key with radius server:
 Server port number: 1812
 Retransmit times: 2
 Request timeout: 5
Console#
```

TACACS+ Client

Terminal Access Controller Access Control System (TACACS+) is a logon authentication protocol that uses software running on a central server to control access to TACACS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user or group that require management access to a switch.

Command	Function	Mode	Page
tacacs-server host	Specifies the TACACS+ server	GC	4-67
tacacs-server port	Specifies the TACACS+ server network port	GC	4-67
tacacs-server key	Sets the TACACS+ encryption key	GC	4-68
show tacacs-server	Shows the current TACACS+ settings	GC	4-68

tacacs-server host

This command specifies the TACACS+ server. Use the **no** form to restore the default.

Syntax

tacacs-server host *host_ip_address*
no tacacs-server host

host_ip_address - IP address of a TACACS+ server.

Default Setting

10.11.12.13

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server host 192.168.1.25
Console(config)#
```

tacacs-server port

This command specifies the TACACS+ server network port. Use the **no** form to restore the default.

Syntax

tacacs-server port *port_number*
no tacacs-server port

port_number - TACACS+ server TCP port used for authentication messages. (Range: 1-65535)

Default Setting

49

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server port 181
Console(config)#
```

tacacs-server key

This command sets the TACACS+ encryption key. Use the **no** form to restore the default.

Syntax

tacacs-server key *key_string*
no tacacs-server key

key_string - Encryption key used to authenticate logon access for the client. Do not use blank spaces in the string.
(Maximum length: 20 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server key green
Console(config)#
```

show tacacs-server

This command displays the current settings for the TACACS+ server.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show tacacs-server
Remote TACACS server configuration:
 Server IP address: 10.11.12.13
 Communication key with radius server: green
 Server port number: 49
Console#
```

Port Security Commands

These commands can be used to disable the learning function or manually specify secure addresses for a port. You may want to leave port security off for an initial training period (i.e., enable the learning function) to register all the current VLAN members on the selected port, and then enable port security to ensure that the port will drop any incoming frames with a source MAC address that is unknown or has been previously learned from another port.

Command	Function	Mode	Page
port security	Configures a secure port	IC	4-69
mac-address-table static	Maps a static address to a port in a VLAN	GC	4-120
show mac-address-table	Displays entries in the bridge-forwarding database	PE	4-121

port security

This command enables or configures port security. Use the **no** form without any keywords to disable port security. Use the **no** form with the appropriate keyword to restore the default settings for a response to security violation or for the maximum number of allowed addresses.

Syntax

port security [**action** {**shutdown** | **trap** | **trap-and-shutdown**}
| **max-mac-count** *address-count*]
no port security [**action** | **max-mac-count**]

- **action** - Response to take when port security is violated.
- **shutdown** - Disable port only.
- **trap** - Issue SNMP trap message only.
- **trap-and-shutdown** - Issue SNMP trap message and disable port.
- max-mac-count *address-count* - The maximum number of MAC addresses that can be learned on a port. (Range: 0 - 20)

Default Setting

Status: Disabled
Action: None
Maximum Addresses: 0

Command Mode

Interface Configuration (Ethernet)

Command Usage

- If you enable port security, the switch will stop dynamically learning new addresses on the specified port. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted.

- To use port security, first allow the switch to dynamically learn the <source MAC address, VLAN> pair for frames received on a port for an initial training period, and then enable port security to stop address learning. Be sure you enable the learning function long enough to ensure that all valid VLAN members have been registered on the selected port.
- To add new VLAN members at a later time, you can manually add secure addresses with the **mac-address-table static** command, or turn off port security to re-enable the learning function long enough for new VLAN members to be registered. Learning may then be disabled again, if desired, for security.
- A secure port has the following restrictions:
  - Cannot use port monitoring.
  - Cannot be a multi-VLAN port.
  - Cannot be connected to a network interconnection device.
  - Cannot be a trunk port.
- If a port is disabled due to a security violation, it must be manually re-enabled using the **no shutdown** command.

Example

The following example enables port security for port 5, and sets the response to a security violation to issue a trap message:

```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap
```

Related Commands

shutdown (4-91)
mac-address-table static (4-120)
show mac-address-table (4-121)

802.1x Port Authentication

The switch supports IEEE 802.1x (dot1x) port-based access control that prevents unauthorized access to the network by requiring users to first submit credentials for authentication. Client authentication is controlled centrally by a RADIUS server using EAP (Extensible Authentication Protocol).

Command	Function	Mode	Page
authentication dot1x default	Sets the default authentication server type	GC	4-71
dot1x default	Resets all dot1x parameters to their default values	GC	4-71
dot1x max-req	Sets the maximum number of times that the switch retransmits an EAP request/identity packet to the client before it times out the authentication session	GC	4-72
dot1x port-control	Sets dot1x mode for a port interface	IC	4-72
dot1x operation-mode	Allows single or multiple hosts on an dot1x port	IC	4-73
dot1x re-authenticate	Forces re-authentication on specific ports	PE	4-73
dot1x re-authentication	Enables re-authentication for all ports	GC	4-74

Command	Function	Mode	Page
dot1x timeout quiet-period	Sets the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client	GC	4-74
dot1x timeout re-authperiod	Sets the time period after which a connected client must be re-authenticated	GC	4-75
dot1x timeout tx-period	Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet	GC	4-75
show dot1x	Shows all dot1x related information	PE	4-76

authentication dot1x default

This command sets the default authentication server type. Use the **no** form to restore the default.

Syntax

authentication dot1x default radius
no authentication dot1x

Default Setting

RADIUS

Command Mode

Global Configuration

Example

```
Console(config)#authentication dot1x default radius
Console(config)#
```

dot1x default

This command sets all configurable dot1x global and port settings to their default values.

Syntax

dot1x default

Command Mode

Global Configuration

Example

```
Console(config)#dot1x default
Console(config)#
```

dot1x max-req

This command sets the maximum number of times the switch port will retransmit an EAP request/identity packet to the client before it times out the authentication session. Use the **no** form to restore the default.

Syntax

dot1x max-req *count*
no dot1x max-req

count – The maximum number of requests (Range: 1-10)

Default

2

Command Mode

Global Configuration

Example

```
Console(config)#dot1x max-req 2
Console(config)#
```

dot1x port-control

This command sets the dot1x mode on a port interface. Use the **no** form to restore the default.

Syntax

dot1x port-control {**auto** | **force-authorized** | **force-unauthorized**}
no dot1x port-control

- **auto** – Requires a dot1x-aware connected client to be authorized by the RADIUS server. Clients that are not dot1x-aware will be denied access.
- **force-authorized** – Configures the port to grant access to all clients, either dot1x-aware or otherwise.
- **force-unauthorized** – Configures the port to deny access to all clients, either dot1x-aware or otherwise.

Default

force-authorized

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x port-control auto
Console(config-if)#
```

dot1x operation-mode

This command allows single or multiple hosts (clients) to connect to an 802.1X-authorized port. Use the **no** form with no keywords to restore the default to single host. Use the **no** form with the **multi-host max-count** keywords to restore the default maximum count.

Syntax

dot1x operation-mode {**single-host** | **multi-host** [**max-count** *count*]}
no dot1x operation-mode [**multi-host max-count**]

- **single-host** – Allows only a single host to connect to this port.
- **multi-host** – Allows multiple host to connect to this port.
- **max-count** – Keyword for the maximum number of hosts.
- *count* – The maximum number of hosts that can connect to a port. (Range: 1-20; Default: 5)

Default

Single-host

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x operation-mode multi-host max-count 10
Console(config-if)#
```

dot1x re-authenticate

This command forces re-authentication on all ports or a specific interface.

Syntax

dot1x re-authenticate *interface*

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.

Command Mode

Privileged Exec

Example

```
Console#dot1x re-authenticate
Console#
```

dot1x re-authentication

This command enables periodic re-authentication globally for all ports. Use the **no** form to disable re-authentication.

Syntax

[**no**] **dot1x re-authentication**

Command Mode

Global Configuration

Example

```
Console(config)#dot1x re-authentication
Console(config)#
```

dot1x timeout quiet-period

This command sets the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client. Use the **no** form to reset the default.

Syntax

dot1x timeout quiet-period *seconds*
no dot1x timeout quiet-period

seconds - The number of seconds. (Range: 1-65535)

Default

60 seconds

Command Mode

Global Configuration

Example

```
Console(config)#dot1x timeout quiet-period 350
Console(config)#
```

dot1x timeout re-authperiod

This command sets the time period after which a connected client must be re-authenticated.

Syntax

dot1x timeout re-authperiod *seconds*
no dot1x timeout re-authperiod

seconds - The number of seconds. (Range: 1-65535)

Default

3600 seconds

Command Mode

Global Configuration

Example

```
Console(config)#dot1x timeout re-authperiod 300
Console(config)#
```

dot1x timeout tx-period

This command sets the time that the switch waits during an authentication session before re-transmitting an EAP packet. Use the **no** form to reset to the default value.

Syntax

dot1x timeout tx-period *seconds*
no dot1x timeout tx-period

seconds - The number of seconds. (Range: 1-65535)

Default

30 seconds

Command Mode

Global Configuration

Example

```
Console(config)#dot1x timeout tx-period 300
Console(config)#
```

show dot1x

This command shows general port authentication related settings on the switch or a specific interface.

Syntax

show dot1x [**statistics**] [**interface** *interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.

Command Mode

Privileged Exec

Command Usage

This command displays the following information:

- *Global 802.1X Parameters* – Displays the global port access control parameters that can be configured for this switch as described in the preceding pages, including reauth-enabled (page 4-74), reauth-period (page 4-75), quiet-period (page 4-74), tx-period (page 4-75), and max-req (page 4-72). It also displays the following global parameters which are set to a fixed value, including the following items:

- supp-timeout	– Supplicant timeout.
- server-timeout	– Server timeout.
- reauth-max	– Maximum number of reauthentication attempts.

- *802.1X Port Summary* – Displays the port access control parameters for each interface, including the following items:

- Status	– Administrative state for port access control.
- Mode	– Dot1x port control mode (page 4-72).
- Authorized	– Authorization status (yes or n/a - not authorized).

- *802.1X Port Details* – Displays detailed port access control settings for each interface as described in the preceding pages, including administrative status for port access control, Max request (page 4-72), Quiet period (page 4-74), Reauth period (page 4-75), Tx period (page 4-75), and Port-control (page 4-72). It also displays the following information:

- Status	– Authorization status (authorized or unauthorized).
- Supplicant	– MAC address of authorized client.

- *Authenticator State Machine*

- State	– Current state (including initialize, disconnected, connecting, authenticating, authenticated, aborting, held, force_authorized, force_unauthorized).
- Reauth Count	– Number of times connecting state is re-entered.

- *Backend State Machine*
  - State – Current state (including request, response, success, fail, timeout, idle, initialize).
  - Request Count – Number of EAP Request packets sent to the Supplicant without receiving a response.
  - Identifier(Server) – Identifier carried in the most recent EAP Success, Failure or Request packet received from the Authentication Server.
- *Reauthentication State Machine*

  State – Current state (including initialize, reauthenticate).

Example

```
Console#show dot1x
Global 802.1X Parameters
 reauth-enabled: yes
 reauth-period:  300
 quiet-period:   350
 tx-period:      300
 supp-timeout:   30
 server-timeout: 30
 reauth-max:     2
 max-req:        2

802.1X Port Summary
 Port Name     Status           Mode           Authorized
        1       disabled    ForceAuthorized            n/a
        2       disabled    ForceAuthorized            n/a
:
       25       disabled    ForceAuthorized            yes
       26        enabled               Auto            yes

802.1X Port Details

802.1X is disabled on port 1
:
802.1X is enabled on port 26
Max request          2
Quiet period         350
Reauth period        300
Tx period            300
Status               Unauthorized
Port-control         Auto
Supplicant           00-00-00-00-00-00

Authenticator State Machine
State                Connecting
Reauth Count         3
Backend State Machine
State                Idle
Request Count        0
Identifier(Server)   0

Reauthentication State Machine
State                Initialize
Console#
```

SNMP Commands

SNMP Commands control access to this switch from management stations using the Simple Network Management Protocol (SNMP), as well as the error types sent to trap managers.

Command	Function	Mode	Page
snmp-server community	Sets up the community access string to permit access to SNMP commands	GC	4-78
snmp-server contact	Sets the system contact string	GC	4-79
snmp-server location	Sets the system location string	GC	4-79
snmp-server host	Specifies the recipient of an SNMP notification operation	GC	4-80
snmp-server enable traps	Enables the device to send SNMP traps (i.e., SNMP notifications)	GC	4-81
snmp ip filter	Sets IP addresses of clients allowed management access to the switch via SNMP	GC	4-82
show snmp	Displays the status of SNMP communications	NE, PE	4-83

snmp-server community

This command defines the community access string for the Simple Network Management Protocol. Use the **no** form to remove the specified community string.

Syntax

snmp-server community *string* [**ro**|**rw**]
no snmp-server community *string*

- *string* - Community string that acts like a password and permits access to the SNMP protocol. (Maximum length: 32 characters, case sensitive; Maximum number of strings: 5)
- **ro** - Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
- **rw** - Specifies read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Default Setting

- public - Read-only access. Authorized management stations are only able to retrieve MIB objects.
- private - Read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Command Mode

Global Configuration

Command Usage

The first snmp-server community command you enter enables SNMP (SNMPv1). The no snmp-server community command disables SNMP.

Example

```
Console(config)#snmp-server community alpha rw
Console(config)#
```

snmp-server contact

This command sets the system contact string. Use the **no** form to remove the system contact information.

Syntax

snmp-server contact *string*
no snmp-server contact

string - String that describes the system contact information. (Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server contact Paul
Console(config)#
```

Related Commands

snmp-server location (4-79)

snmp-server location

This command sets the system location string. Use the **no** form to remove the location string.

Syntax

snmp-server location *text*
no snmp-server location

text - String that describes the system location. (Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server location WC-19
Console(config)#
```

Related Commands

snmp-server contact (4-79)

snmp-server host

This command specifies the recipient of a Simple Network Management Protocol notification operation. Use the **no** form to remove the specified host.

Syntax

snmp-server host *host-addr community-string* [**version** {**1** | **2c**}]
no snmp-server host *host-addr*

- *host-addr* - Internet address of the host (the targeted recipient). (Maximum host addresses: 5 trap destination IP address entries)
- *community-string* - Password-like community string sent with the notification operation. Although you can set this string using the **snmp-server host** command by itself, we recommend that you define this string using the **snmp-server community** command prior to using the **snmp-server host** command. (Maximum length: 32 characters)
- **version** - Specifies whether to send notifications as SNMP v1 or v2c traps.

Default Setting

Host Address: None
SNMP Version: 1

Command Mode

Global Configuration

Command Usage

- If you do not enter an **snmp-server host** command, no notifications are sent. In order to configure the switch to send SNMP notifications, you must enter at least one **snmp-server host** command. In order to enable multiple hosts, you must issue a separate **snmp-server host** command for each host.
- The **snmp-server host** command is used in conjunction with the **snmp-server enable traps** command. Use the **snmp-server enable traps** command to specify which SNMP notifications are sent globally. For a host to receive notifications, at least one **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled.
- Some notification types cannot be controlled with the **snmp-server enable traps** command. For example, some notification types are always enabled.
- The switch can send SNMP version 1 or version 2c notifications to a host IP address, depending on the SNMP version that the management station supports. If the snmp-server host command does not specify the SNMP version, the default is to send SNMP version 1 notifications.

Example

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#
```

Related Commands

snmp-server enable traps (4-81)

snmp-server enable traps

This command enables this device to send Simple Network Management Protocol traps (SNMP notifications). Use the **no** form to disable SNMP notifications.

Syntax

[**no**] **snmp-server enable traps** [**authentication** | **link-up-down**]

- **authentication** - Keyword to issue authentication failure traps.
- **link-up-down** - Keyword to issue link-up or link-down traps.
  The link-up-down trap can only be enabled/disabled via the CLI.

Default Setting

Issue authentication and link-up-down traps.

Command Mode

Global Configuration

Command Usage

- If you do not enter an **snmp-server enable traps** command, no notifications controlled by this command are sent. In order to configure this device to send SNMP notifications, you must enter at least one **snmp-server enable traps** command. If you enter the command with no keywords, both authentication and link-up-down notifications are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled.
- The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one **snmp-server host** command.

Example

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

Related Commands

snmp-server host (4-80)

snmp ip filter

This command sets the IP addresses of clients that are allowed management access to the switch via SNMP. Use the **no** form the remove an IP address.

Syntax

[**no**] **snmp ip filter** *ip_address subnet_mask*

- *ip_address* - An IP address indicating a client or group of clients that are allowed SNMP access to the switch.
- *subnet_mask* - An address bitmask of decimal numbers that represent the address bits to match.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- You can create a list of up to 16 IP addresses or IP address groups that are allowed access to the switch via SNMP management software.
- Address bitmasks are similar to a subnet mask, containing four decimal integers from 0 to 255, each separated by a period. The binary mask uses “1” bits to indicate “match” and “0” bits to indicate “ignore.”
- If the IP is the address of a single management station, the bitmask should be set to 255.255.255.255. Otherwise, an IP address group is specified by the bitmask.
- The default setting is null, which allows all IP groups SNMP access to the switch. If one IP address is configured, IP filtering is enabled and only addresses in the specified IP group will have SNMP access.
- IP filtering does not affect management access to the switch using the Web interface or Telnet.

Example

The following example enables SNMP IP filtering on the switch and allows SNMP management access to client IP 10.1.2.3, and client IP group 10.1.3.0 to 10.1.3.255.

```
Console(config)#snmp ip filter 10.1.2.3 255.255.255.255
Console(config)#snmp ip filter 10.1.3.0 255.255.255.0
Console(config)#
```

Related Commands

show snmp (4-83)

show snmp

This command checks the status of SNMP communications.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command provides information on the community access strings, counter information for SNMP input and output protocol data units, and whether or not SNMP logging has been enabled with the snmp-server enable traps command.

Example

```
Console#show snmp

SNMP traps:
 Authentication: enable
   Link-up-down: enable

SNMP communities:
   1. private, and the privilege is read-write
   2. public, and the privilege is read-only

0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
0 SNMP packets output
    0 Too big errors
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs

SNMP logging: disabled
SNMP ip filter group:
Console#
```

DHCP Commands

These commands are used to configure Dynamic Host Configuration Protocol (DHCP) client. You can configure any VLAN interface to be automatically assigned an IP address via DHCP.

DHCP Client

Command	Function	Mode	Page
ip dhcp client-identifier	Specifies the DHCP client identifier for this switch	IC	4-84
ip dhcp restart client	Submits a BOOTP or DHCP client request	PE	4-85

ip dhcp client-identifier

This command specifies the DCHP client identifier for the current interface. Use the **no** form to remove this identifier.

Syntax

ip dhcp client-identifier {**text** *text* | **hex** *hex*}
no ip dhcp client-identifier

- *text* - A text string. (Range: 1-15 characters)
- *hex* - The hexadecimal value.

Default Setting

None

Command Mode

Interface Configuration (VLAN)

Command Usage

This command is used to include a client identifier in all communications with the DHCP server. The identifier type depends on the requirements of your DHCP server.

Example

```
Console(config)#interface vlan 2
Console(config-if)#ip dhcp client-identifier hex 00-00-e8-66-65-72
Console(config-if)#
```

Related Commands

ip dhcp restart client (4-85)

ip dhcp restart client

This command submits a BOOTP or DHCP client request.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- This command issues a BOOTP or DHCP client request for any IP interface that has been set to BOOTP or DHCP mode via the **ip address** command.
- DHCP requires the server to reassign the client's last address if available.
- If the BOOTP or DHCP server has been moved to a different domain, the network portion of the address provided to the client will be based on this new domain.

Example

In the following example, the device is reassigned the same address.

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#exit
Console#ip dhcp restart client
Console#show ip interface
 IP address and netmask: 192.168.1.54 255.255.255.0 on VLAN 1,
 and address mode: Dhcp.
Console#
```

Related Commands

ip address (4-165)

Interface Commands

These commands are used to display or set communication parameters for an Ethernet port, aggregated link, or VLAN.

Command	Function	Mode	Page
interface	Configures an interface type and enters interface configuration mode	GC	4-86
description	Adds a description to an interface configuration	IC	4-87
speed-duplex	Configures the speed and duplex operation of a given interface when autonegotiation is disabled	IC	4-87
negotiation	Enables autonegotiation of a given interface	IC	4-88
capabilities	Advertises the capabilities of a given interface for use in autonegotiation	IC	4-89
flowcontrol	Enables flow control on a given interface	IC	4-90
combo-forced-mode	Force port type selected for combination ports	IC	4-91
shutdown	Disables an interface	IC	4-91
switchport broadcast packet-rate	Configures the broadcast storm control threshold	IC	4-91
clear counters	Clears statistics on an interface	PE	4-92
show interfaces status	Displays status for the specified interface	NE, PE	4-93
show interfaces counters	Displays statistics for the specified interfaces	NE, PE	4-94
show interfaces switchport	Displays the administrative and operational status of an interface	NE, PE	4-95

interface

This command configures an interface type and enter interface configuration mode. Use the **no** form to remove a trunk.

Syntax

interface *interface*
no interface port-channel *channel-id*

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Value: 1)
- **vlan** *vlan-id* (Range: 1-4093)

Default Setting

None

Command Mode

Global Configuration

Example

To specify port 24, enter the following command:

```
Console(config)#interface ethernet 1/24
Console(config-if)#
```

description

This command adds a description to an interface. Use the **no** form to remove the description.

Syntax

description *string*
no description

string - Comment or a description to help you remember what is attached to this interface. (Range: 1-64 characters)

Default Setting

None

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

The following example adds a description to port 2.

```
Console(config)#interface ethernet 1/2
Console(config-if)#description RD-SW#3
Console(config-if)#
```

speed-duplex

This command configures the speed and duplex mode of a given interface when autonegotiation is disabled. Use the **no** form to restore the default.

Syntax

speed-duplex {**1000full** | **100full** | **100half** | **10full** | **10half**}
no speed-duplex

- **1000full** - Forces 1000 Mbps full-duplex operation
- **100full** - Forces 100 Mbps full-duplex operation
- **100half** - Forces 100 Mbps half-duplex operation
- **10full** - Forces 10 Mbps full-duplex operation
- **10half** - Forces 10 Mbps half-duplex operation

Default Setting

- Auto-negotiation is enabled by default.
- When auto-negotiation is disabled, the default speed-duplex setting is 100half for 100BASE-TX ports and 1000full for Gigabit Ethernet ports.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- To force operation to the speed and duplex mode specified in a **speed-duplex** command, use the **no negotiation** command to disable auto-negotiation on the selected interface.
- When using the **negotiation** command to enable auto-negotiation, the optimal settings will be determined by the **capabilities** command. To set the speed/ duplex mode under auto-negotiation, the required mode must be specified in the capabilities list for an interface.

Example

The following example configures port 5 to 100 Mbps, half-duplex operation.

```
Console(config)#interface ethernet 1/5
Console(config-if)#speed-duplex 100half
Console(config-if)#no negotiation
Console(config-if)#
```

Related Commands

negotiation (4-88)
capabilities (4-89)

negotiation

This command enables autonegotiation for a given interface. Use the **no** form to disable autonegotiation.

Syntax

[**no**] **negotiation**

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- When auto-negotiation is enabled the switch will negotiate the best settings for a link based on the **capabilities** command. When auto-negotiation is disabled, you must manually specify the link attributes with the **speed-duplex** and **flowcontrol** commands.
- If autonegotiation is disabled, auto-MDI/MDI-X pin signal configuration will also be disabled for the RJ-45 ports.

Example

The following example configures port 11 to use autonegotiation.

```
Console(config)#interface ethernet 1/11
Console(config-if)#negotiation
Console(config-if)#
```

Related Commands

capabilities (4-89)
speed-duplex (4-87)

capabilities

This command advertises the port capabilities of a given interface during autonegotiation. Use the **no** form with parameters to remove an advertised capability, or the **no** form without parameters to restore the default values.

Syntax

[**no**] **capabilities** {**1000full** | **100full** | **100half** | **10full** | **10half** | **flowcontrol** | **symmetric**}

- **1000full** - Supports 1000 Mbps full-duplex operation
- **100full** - Supports 100 Mbps full-duplex operation
- **100half** - Supports 100 Mbps half-duplex operation
- **10full** - Supports 10 Mbps full-duplex operation
- **10half** - Supports 10 Mbps half-duplex operation
- **flowcontrol** - Supports flow control
- **symmetric** (Gigabit only) - When specified, the port transmits and receives pause frames; when not specified, the port will auto-negotiate to determine the sender and receiver for asymmetric pause frames. (*The current switch ASIC only supports symmetric pause frames.*)

Default Setting

- 1000BASE-T: 10half, 10full, 100half, 100full, 1000full
- 1000BASE-SX/LX/LH: 1000full

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

When auto-negotiation is enabled with the negotiation command, the switch will negotiate the best settings for a link based on the capabilites command. When auto-negotiation is disabled, you must manually specify the link attributes with the speed-duplex and flowcontrol commands.

Example

The following example configures Ethernet port 5 capabilities to 100half, 100full and flow control.

```
Console(config)#interface ethernet 1/5
Console(config-if)#capabilities 100half
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
Console(config-if)#
```

Related Commands

negotiation (4-88)
speed-duplex (4-87)
flowcontrol (4-90)

flowcontrol

This command enables flow control. Use the **no** form to disable flow control.

Syntax

[**no**] **flowcontrol**

Default Setting

Flow control enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Flow control can eliminate frame loss by “blocking” traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3x for full-duplex operation.
- To force flow control on or off (with the **flowcontrol** or **no flowcontrol** command), use the **no negotiation** command to disable auto-negotiation on the selected interface.
- When using the **negotiation** command to enable auto-negotiation, the optimal settings will be determined by the **capabilities** command. To enable flow control under auto-negotiation, “flowcontrol” must be included in the capabilities list for any port
- Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.

Example

The following example enables flow control on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#flowcontrol
Console(config-if)#no negotiation
Console(config-if)#
```

Related Commands

negotiation (4-88)
capabilities (4-89)

shutdown

This command disables an interface. To restart a disabled interface, use the **no** form.

Syntax

[**no**] **shutdown**

Default Setting

All interfaces are enabled.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This command allows you to disable a port due to abnormal behavior (e.g., excessive collisions), and then reenable it after the problem has been resolved. You may also want to disable a port for security reasons.

Example

The following example disables port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#shutdown
Console(config-if)#
```

switchport broadcast packet-rate

This command configures broadcast storm control. Use the **no** form to disable broadcast storm control.

Syntax

switchport broadcast packet-rate *rate*
no switchport broadcast

rate - Threshold level as a rate; i.e., packets per second. (Range: 500 - 262143)

Default Setting

Enabled for all ports
Packet-rate limit: 500 packets per second

Command Mode

Interface Configuration (Ethernet)

Command Usage

- When broadcast traffic exceeds the specified threshold, packets above that threshold are dropped.
- This command can enable or disable broadcast storm control for the selected interface. However, the specified threshold value applies to all ports on the switch.

Example

The following shows how to configure broadcast storm control at 600 packets per second:

```
Console(config)#interface ethernet 1/5
Console(config-if)#switchport broadcast packet-rate 600
Console(config-if)#
```

clear counters

This command clears statistics on an interface.

Syntax

clear counters *interface*

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Value: 1)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Statistics are only initialized for a power reset. This command sets the base value for displayed statistics to zero for the current management session. However, if you log out and back into the management interface, the statistics displayed will show the absolute value accumulated since the last power reset.

Example

The following example clears statistics on port 5.

```
Console#clear counters ethernet 1/5
Console#
```

show interfaces status

This command displays the status for an interface.

Syntax

show interfaces status [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Value: 1)
- **vlan** *vlan-id* (Range: 1-4093)

Default Setting

Shows the status for all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed. For a description of the items displayed by this command, see “Displaying Connection Status” on page 3-40.

Example

```
Console#show interfaces status ethernet 1/1
Information of Eth 1/1
 Basic information:
  Port type: 100TX-EFM
  Mac address: 00-01-00-02-00-04
 Configuration:
  Name:
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full,
  Broadcast storm: Enabled
  Broadcast storm limit: 650 packets/second
  Flow control: Disabled
  Lacp: Disabled
  Port security: Disabled
  Max MAC count: 0
  Port security action: None
 Current status:
  Link status: Up
  Port operation status: Up
  Operation speed-duplex: 100full
  Flow control type: None
Console#
```

show interfaces counters

This command displays interface statistics.

Syntax

show interfaces counters [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1
  - *port* - Port number
- **port-channel** *channel-id* (Value: 1)

Default Setting

Shows the counters for all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed. For a description of the items displayed by this command, see “Showing Port Statistics” on page 3-51.

Example

```
Ethernet 1/ 1
 Iftable stats:
  Octets input: 113404, Octets output: 742007
  Unicast input: 739, Unicast output: 836
  Discard input: 0, Discard output: 0
  Error input: 0, Error output: 0
  Unknown protos input: 0, QLen output: 0
 Extended iftable stats:
  Multi-cast input: 482, Multi-cast output: 9
  Broadcast input: 38, Broadcast output: 0
 Ether-like stats:
  Alignment errors: 0, FCS errors: 0
  Single Collision frames: 0, Multiple collision frames: 0
  SQE Test errors: 0, Deferred transmissions: 0
  Late collisions: 0, Excessive collisions: 0
  Internal mac transmit errors: 0, Internal mac receive errors: 0
  Frame too longs: 0, Carrier sense errors: 0
  Symbol errors: 0
 RMON stats:
  Drop events: 0, Octets: 855411, Packets: 2104
  Broadcast pkts: 38, Multi-cast pkts: 491
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
 CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets: 1332, Packet size 65 to 127 octets: 123
  Packet size 128 to 255 octets: 15, Packet size 256 to 511 octets: 142
  Packet size 512 to 1023 octets: 9, Packet size 1024 to 1518 octets: 483
Console#
```

Related Commands

show controllers ethernet-controller (4-110)

show interfaces switchport

This command displays the administrative and operational status of the specified interfaces.

Syntax

show interfaces switchport [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Value: 1)

Default Setting

Shows all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed.

Example

This example shows the configuration setting for port 2.

```
Console#show interfaces switchport ethernet 1/2
Information of Eth 1/2
 Broadcast threshold: Enabled, 650 packets/second
 Lacp status: Disabled
 Ingress rate limit: disable,100M bits per second
 Egress rate limit: disable,100M bits per second
 VLAN membership mode: Hybrid
 Ingress rule: Disabled
 Acceptable frame type: All frames
 Native VLAN: 1
 Priority for untagged traffic: 0
 Gvrp status: Disabled*
 Allowed Vlan:    1(u),
 Forbidden Vlan:
Console#
```

* Not supported in the present version

Field	Description
Broadcast threshold	Shows if broadcast storm suppression is enabled or disabled; if enabled it also shows the threshold level (page 4-91).
Lacp status	Shows if Link Aggregation Control Protocol has been enabled or disabled (page 4-101).
Ingress/Egress rate limit	Shows if rate limiting is enabled, and the current rate limit. (page 4-99).
VLAN membership mode	Indicates membership mode as Trunk or Hybrid (page 4-138).
Ingress rule	Shows if ingress filtering is enabled or disabled (page 4-139).
Acceptable frame type	Shows if acceptable VLAN frames include all types or tagged frames only (page 4-138).
Native VLAN	Indicates the default Port VLAN ID (page 4-140).
Priority for untagged traffic	Indicates the default priority for untagged frames (page 4-145).
Allowed Vlan	Shows the VLANs this interface has joined, where “(u)” indicates untagged and “(t)” indicates tagged (page 4-140).
Forbidden Vlan	Shows the VLANs this interface cannot dynamically join via GVRP.*

* Not supported in the current version

Mirror Port Commands

This section describes how to mirror traffic from a source port to a target port.

Command	Function	Mode	Page
port monitor	Configures a mirror session	IC	4-97
show port monitor	Shows the configuration for a mirror port	PE	4-98

port monitor

This command configures a mirror session. Use the **no** form to clear a mirror session.

Syntax

port monitor *interface* [**rx** | **tx** | **both**]
no port monitor *interface*

interface

- **ethernet** *unit*/*port* (source port)
  - *unit* - Switch (unit 1)
  - *port* - Port number
- **rx** - Mirror received packets.
- **tx** - Mirror transmitted packets.
- **both** - Mirror both received and transmitted packets.

Default Setting

No mirror session is defined. When enabled, the default mirroring is for both received and transmitted packets.

Command Mode

Interface Configuration (Ethernet, destination port)

Command Usage

- You can mirror traffic from any source port to a destination port for real-time analysis. You can then attach a logic analyzer or RMON probe to the destination port and study the traffic crossing the source port in a completely unobtrusive manner.
- The destination port is set by specifying an Ethernet interface.
- The mirror port and monitor port speeds should match, otherwise traffic may be dropped from the monitor port.
- You can create multiple mirror sessions, but all sessions must share the same destination port. However, you should avoid sending too much traffic to the destination port from multiple source ports.

Example

The following example configures the switch to mirror all packets from port 6 to 11:

```
Console(config)#interface ethernet 1/11
Console(config-if)#port monitor ethernet 1/6 both
Console(config-if)#
```

show port monitor

This command displays mirror information.

Syntax

show port monitor [*interface*]

interface - **ethernet** *unit*/*port* (source port)

- *unit* - Switch (unit 1)
- *port* - Port number

Default Setting

Shows all sessions.

Command Mode

Privileged Exec

Command Usage

This command displays the currently configured source port, destination port, and mirror mode (i.e., RX, TX, RX/TX).

Example

The following shows mirroring configured from port 6 to port 11:

```
Console(config)#interface ethernet 1/11
Console(config-if)#port monitor ethernet 1/6
Console(config-if)#end
Console#show port monitor
Port Mirroring
-------------------------------------
 Destination port(listen port):Eth1/1
 Source port(monitored port)  :Eth1/6
 Mode                         :RX/TX
Console#
```

Rate Limit Commands

This function allows the network manager to control the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports or trunks. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped, conforming traffic is forwarded without any changes.

Command	Function	Mode	Page
rate-limit	Configures the maximum input or output rate for a port	IC	4-99

rate-limit

This command defines the rate limit for a specific interface. Use this command without specifying a rate to restore the default rate. Use the **no** form to restore the default status of disabled.

Syntax

rate-limit {**input** | **output**} [*rate*]
no rate-limit {**input** | **output**}

- **input** – Input rate
- **output** – Output rate
- *rate* – Maximum value in Mbps. (Range: 100 Mbps for ports 1-12, 1000 Mbps for ports 13-14 with Gigabit modules installed)

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#rate-limit input 600
Console(config-if)#
```

Link Aggregation Commands

Ports can be statically grouped into an aggregate link (i.e., trunk) to increase the bandwidth of a network connection or to ensure fault recovery. Or you can use the Link Aggregation Control Protocol (LACP) to automatically negotiate a trunk link between this switch and another network device. For static trunks, the switches have to comply with the Cisco EtherChannel standard. For dynamic trunks, the switches have to comply with LACP. This switch supports up to six trunks. For example, a trunk consisting of two 1000 Mbps ports can support an aggregate bandwidth of 4 Gbps when operating at full duplex.

Command	Function	Mode	Page
Manual Configuration Commands			
interface port-channel	Configures a trunk and enters interface configuration mode for the trunk	GC	4-86
channel-group	Adds a port to a trunk	IC (Ethernet)	4-101
Dynamic Configuration Command			
lacp	Configures LACP for the current interface	IC (Ethernet)	4-101
Trunk Status Display Command			
show interfaces status port-channel	Shows trunk information	NE, PE	4-93
show lacp	Shows LACP information	PE	4-101

Guidelines for Creating Trunks

General Guidelines –

- Finish configuring port trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- A trunk can have two Gigabit optional module ports.
- The ports at both ends of a connection must be configured as trunk ports.
- All ports in a trunk must be configured in an identical manner, including communication mode (i.e., speed, duplex mode and flow control), VLAN assignments, and CoS settings.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN via the specified port-channel.
- STP, VLAN, and IGMP settings can only be made for the entire trunk via the specified port-channel.

Dynamically Creating a Port Channel –

Ports assigned to a common port channel must meet the following criteria:

- Ports must have the same LACP system priority.
- Ports must have the same port admin key (Ethernet Interface).
- If the port channel admin key (lacp admin key - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key (lacp admin key - Ethernet Interface) used by the interfaces that joined the group.

- However, if the port channel admin key is set, then the port admin key must be set to the same value for a port to be allowed to join a channel group.
- If a link goes down, LACP port priority is used to select the backup link.

channel-group

This command adds a port to a trunk. Use the **no** form to remove a port from a trunk.

Syntax

channel-group *channel-id*
no channel-group

channel-id - Trunk index (Value: 1)

Default Setting

The current port will be added to this trunk.

Command Mode

Interface Configuration (Ethernet)

Command Usage

- When configuring static trunks, the switches must comply with the Cisco EtherChannel standard.
- Use **no channel-group** to remove a port group from a trunk.
- Use **no interfaces port-channel** to remove a trunk from the switch.

Example

The following example creates trunk 1 and then adds port 13:

```
Console(config)#interface port-channel 1
Console(config-if)#exit
Console(config)#interface ethernet 1/13
Console(config-if)#channel-group 1
Console(config-if)#
```

lacp

This command enables 802.3ad Link Aggregation Control Protocol (LACP) for the current interface. Use the **no** form to disable it.

Syntax

[**no**] **lacp**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

- The ports on both ends of an LACP trunk must be configured for full duplex, either by forced mode or auto-negotiation.
- A trunk formed with another switch using LACP will automatically be assigned the next available port-channel ID.
- If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.
- If more than four ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.

Example

The following shows LACP enabled on ports 13-14. Because LACP has also been enabled on the ports at the other end of the links, the **show interfaces status port-channel 1** command shows that Trunk1 has been established.

```
Console(config)#interface ethernet 1/13
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet 1/14
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#exit
Console#show interfaces status port-channel 1
Information of Trunk 1
 Basic information:
  Port type: 1000GBIC
  Mac address: 00-00-e8-00-00-0b
 Configuration:
  Name:
  Port admin status: Up
  Speed-duplex: Auto
  Capabilities: 1000full,
  Flow control status: Disabled
  Port security: Disabled
  Max MAC count: 0
 Current status:
  Created by: lacp
  Link status: Up
  Port operation status: Up
  Operation speed-duplex: 1000full
  Flow control type: None
  Member Ports: Eth1/13, Eth1/14,
Console#
```

VDSL Commands

These commands are used to to configure and display communication parameters for VDSL and ethernet ports on the switch and connected CPEs.

Command	Function	Mode	Page
efm profile global	Batch assigns profiles for speed to all the VDSL ports on the switch	GC	4-103
efm profile	Assigns profiles for speed to individual VDSL ports	IC	4-105
efm reset	Resets the switch VDSL chipset or, if a CPE is connected, the CPE VDSL chipset	IC	4-106
efm shutdown	Disables the VDSL chipset transmitter of an EFM port that not being used	PE	4-106
efm rdl	Enables/disables Remote Digital Loopback (RDL) mode	IC	4-107
efm interleave	Sets the interleave parameters for the selected port	IC	4-108
efm noise-margin	Sets the noise margin of the selected VDSL port		4-109
efm rate-adapt	Enables and disables the rate adaption feature on the selected VDSL port		4-109
efm pbo	Enables and disables power back-off on the selected VDSL port	IC	4-110
show controllers ethernet-controller	Displays the Ethernet link transmit and receive statistics on a specific VDSL port.	PE	4-110
show controllers efm interface-id actual	Displays the current values of the VDSL link on a specific VDSL port.	PE	4-113
show controllers efm interface-id admin	Displays the administrative settings of the VDSL link on a specific VDSL port	PE	4-114
show controllers efm profile	Displays information about the Ethernet in the First Mile (EFM) profiles available on the switch, and how they are assigned to the VDSL ports	PE	4-114
show controllers efm status	Displays the VDSL link statistics and profile information on a specific VDSL port	PE	4-116
show controllers efm remote ethernet mode	Displays the connected CPE ethernet mode	PE	4-117
show controllers efm-noise-margin	Displays the noise margin for the selected port	PE	4-118
show controllers efm channel-performance	Displays the channel performance for the channels in a VDSL line	PE	4-119

efm profile global

Use this command to batch assign profiles for speed to all the VDSL ports on the switch.

Syntax

efm profile global *profile name*

profile name - Name of the profile.

Default Setting

Default Profile

Command Mode

Global Configuration

Command Usage

Assigns the same profile to each VDSL switch port. Details of these profiles are given in the table below.

Profile Name	ProfileType	Downstream Rate (Mbps)	Upstream Rate (Mbps)
Default	Public	1.20	1.40
A1-02OAG-R1	Public	7.56	2.43
A2-02OAG-R1	Public	10.80	2.43
A3-01OAG-R1	Public	17.28	3.78
A4-01OAG-R1	Public	25.92	4.72
S1-03OAG-R1	Public	7.56	7.56
S2-03OAG-R1	Public	10.80	10.40
S3-00OAG-R1	Public	17.28	16.47
S1-16-16	Private	16.74	16.20
S2-16-16A	Private	16.74	16.20
A1-34-11	Private	33.75	11.34
A2-34-11A	Private	33.75	11.34
A3-25-3	Private	25.38	3.24
A4-45-5	Private	44.55	5.13
A5-50-7	Private	50.47	7.29
A6-22-3A	Private	22.55	3.24
A7-40-5A	Private	40.91	5.13
A8-46-7A	Private	46.44	7.29
TLAN	Private	17.01	5.40
Max-Rate	Private	71.28	40.50

Notes:

1. The VDSL Intelligent Switch uses Ethernet in the First Mile (EFM), a VDSL-based technology.
2. A suffix of “A” in the profile name (e.g., S2-16-16A) indicate that this profile is for both VDSL and ADSL lines in a bundle. Profiles without a suffix of “A” in the profile name (e.g., S1-16-16) are for VDSL lines only.
3. The following profiles are recommended for use with this switch; S1-16-16, S2-16-16A, A1-34-11, and- A2-34-11A.

4. The maximum distances for VDSL links using the recommended profiles are:

Upstream	Downstream	Mode	Max. Range
16 Mbps	16 Mbps	Symetric	600m (1970 ft)
11 Mbps	34 Mbps	Asymetric	610m (2000 ft)

5. Type-1 26 AWG (100 ohm)/0.4 mm, or Type-2 24 AWG (100 ohm)/0.5 mm cable may be installed to achieve the maximum distance, however, typically, 24 AWG (100 ohm)/0.5 mm wire is better than 26 AWG (100 ohm)/0.4 mm wire. Note that the distance may be limited by factors such as how the cable is bundled, and the interference and noise on the link.

6. Public profiles conform to specific standards such as ANSI or ETSI. Private profiles do not conform to these standards.

Example

```
Console#config
Console(config)#efm profile global S1-16-16
Console(config)#
```

Related Commands

efm profile (4-105)

efm profile

Use this command to assign profiles for speed to a specific VDSL port on the switch.

Syntax

efm profile *profile name*

profile name - Name of the profile.

Default Setting

None

Command Mode

Interface Configuration

Command Usage

Assigns a profile to a specific VDSL port. For details of the these profiles see the table under Command Usage for efm profile global.

Example

The following example shows EFM profile S1-16-16 assigned to VDSL port 1.

```
Console#config
Console(config)#interface ethernet 1/1
Console(config-if)#efm profile S1-16-16
Console(config-if)#
```

Related Commands

efm profile global (4-103)

efm reset

Use the efm reset interface configuration command to reset the switch VDSL chipset or, if a CPE is connected, the CPE VDSL chipset.

Syntax

efm reset {**local** | **remote**}

- *local* - Resets the CO side VDSL chipset for a VDSL port.
- *remote* - Resets the CPE side VDSL chipset of a VDSL port.

Default Setting

None

Command Mode

Interface Configuration

Command Usage

Use this command to troubleshoot VDSL port performance.

Example

The following example resets the CO side VDSL and CPE side VDSL chipset of VDSL port 1

```
Console#config
Console(config)#interface ethernet 1/1
Console(config-if)#efm reset local
Console(config-if)#efm reset remote
Console(config-if)#
```

efm shutdown

Use this command to disable a VDSL interface. To enable a disabled interface, use the **no** form.

Syntax

[**no**] **efm shutdown**

Default Setting

All interfaces are enabled.

Command Mode

Interface Configuration

Command Usage

Use this command to disable the VDSL chipset transmitter of a VDSL port that is not connected to a working CPE. In some unusual circumstances, the power emitted by VDSL ports can affect other VDSL ports. It is recommended that ports that are not wired to CPEs be shutdown in this way. Also use this command to disable access to the switch from this port.

Example

The following example disables VDSL port 1.

```
Console (config)#interface ethernet 1/1
Console(config-if)#efm shutdown
Console(config-if)#
```

Related Commands

shutdown (4-91)

efm rdl

Use the efm rdl interface configuration command to enable Remote Digital Loopback (RDL) to disable use the no form of the command.

Syntax

efm rdl
no efm rdl

Default Setting

Off

Command Mode

Interface Configuration

Command Usage

Remote Digital Loopback (RDL) tests the link between the switch and the CPE by sending out, and returning data through the CPE, over the VDSL link.

Example

The following example shows how to turn enable/disable RDL on VDSL port 1.

```
Console (config)#interface ethernet 1/1
Console(config-if)#efm rdl
Console(config-if)#no efm rdl
Console(config-if)#
```

efm interleave

This command sets the interleave parameters for the selected VDSL port.

Syntax

efm interleave [*downstream M value*] [*upstream M value*] [*downstream I value*] [*upstream I value*]

no efm interleave

- *M value* – M is the interleaving depth index; Range: 0-64
- *I value* – I is the interleaving block length; Range: 4 or 8

Default Setting

- M – The interleaving depth index.
  Upstream default value: 8, Downstream default value: 16
- I – The interleaving block length.
  Upstream default value: 8, Downstream default value: 8

Command Mode

Interface Configuration

Command Usage

Interleaving improves Reed Solomon error correction when there is pulse noise. A greater degree of interleaving will provide more protection against pulse noise but will increase transmission delay and reduce the effective bandwidth of the link. The degree of interleaving can be increased by increasing M or I.

Example

The following example configures VDSL port 1 with –

- M - downstream value: 16, Upstream value: 8
- I - downstream value: 8, Upstream value: 8

```
Console#config
Console(config)#interface ethernet 1/1
Console(config-if)#efm interleave 16 8 8 8
Console(config-if)#end
Console#show controllers efm status link Ethernet 1/1
Interface      Link       SNR (dB)         RS Errs        Interleaver
                      DS1  DS2  US1  US2           DS.M DS.I US.M US.I PBO
-------------  ----  --------------------  --------  -------------------
---
Ethernet 1/1   Up     43.0 35.0 45.0 43.0  0          16    8    8    8  on
Console#
```

Related Commands

efm noise-margin (4-109)
show controllers efm status (4-116)

efm noise-margin

This command sets the noise margin of the selected VDSL port.

Syntax

efm noise-margin [*downstream noise margin*] [*upstream noise margin*]
no efm noise-margin

- *downstream noise margin* - Range 0-9
- *upstream noise margin* - Range 0-9

Default Setting

0

Command Mode

Interface Configuration

Command Usage

The noise margin indicates how much the noise on the selected VDSL can increase before the signal is affected. As the noise on the line increases, the margin will approach zero. If the noise exceeds the current noise margin, the signal will be lost. You will then need to increase the margin until the signal is restored.

Example

The following example configures VDSL port 1 with an upstream noise margin of 6 , and a downstream margin of 6.

```
Console(config)#interface ethernet 1/1
Console(config-if)#efm noise-margin 6 6
Console(config-if)#end
```

Related Commands

efm interleave (4-108)
show controllers efm-noise-margin (4-118)

efm rate-adapt

This command enables and disables the rate adaption feature on the selected VDSL port. The data rate on a VDSL line can be affected by factors such as temperature, humidity, and electro-magnetic radiation. When rate adaption is enabled, the switch will determine the optimal transmission rate for the current conditions.

Syntax

efm rate-adapt
no efm rate-adapt

Default Setting

Disabled

Command Mode

Interface Configuration

Command Usage

The data rate on a VDSL line can be affected by factors such as temperature, humidity, and electro-magnetic radiation. When rate adaption is enabled, the switch will determine the optimal transmission rate for the current conditions.

Example

The following example shows rate adaption enabled for port 1.

```
onsole#config
Console(config)#interface ethernet 1/1
Console(config-if)#efm rate-adapt
Console(config-if)#
```

Related Commands

rate-limit (4-99)

efm pbo

This command enables and disables power back-off on the selected VDSL port.

Syntax

[**no**] **efm pbo**

Default Setting

Enabled

Command Mode

Interface Configuration

Command Usage

If PBO is enabled the power of transmission from the port will automatically be adjusted to ensure that the signal successfully reaches the reception port.

Example

The following example shows power back-off enabled for port 1.

```
onsole#config
Console(config)#interface ethernet 1/1
Console(config-if)#efm pbo
Console(config-if)#
```

Related Commands

show controllers efm status (4-116)

show controllers ethernet-controller

Use this command to display the Ethernet link transmit and receive statistics for a specific VDSL port, or for all the VDSL ports on the switch and the connected CPE.

Syntax

show controllers ethernet-controller *interface-id*

interface-id - ID of the VDSL port

Default Setting

None

Command Mode

Privileged EXEC

Command Usage

Using the show controllers ethernet-controller command without specifying a VDSL port displays the Ethernet link statistics of all ports on the switch and on the connected CPE devices. The output shows the statistics collected by the VDSL chipset on the switch, and the statistics collected by the VDSL chipset on the CPE.

Example

```
Console#show controllers ethernet-controller ethernet 1/2
Ethernet 1/2 :
EFM PHY on Switch:
Transmit
   9671624 Bytes Transmitted
      8487 Frames Transmitted
         0 Pause frames
         0 Single Collision Frames
         0 Multiple collisions
         0 Late collisions
         0 Excessive collisions
         0 Deferred frames
         0 Carrier sense errors

Receive
   1406434 Bytes Received
     17551 Frames Received
         0 Broadcast frames
         0 Pause frames
         0 Alignment errors
         0 Collisions and Runts
         0 Oversize frames
         0 FCS errors

EFM MAC on CPE:
Transmit
         0 Bytes Transmitted
         0 Frames Transmitted
         0 Pause frames
         0 Single Collision Frames
         0 Multiple collisions
         0 Late collisions
         0 Excessive collisions
         0 Deferred frames
         0 Carrier sense errors

Receive
         0 Bytes Received
         0 Frames Received
         0 Broadcast frames
         0 Pause frames
         0 Alignment errors
         0 Collisions and Runts
         0 Oversize frames
         0 FCS errors
Console#
```

Related Commands

show interfaces counters (4-94)

show controllers efm actual

Use this command to display the current values of the VDSL link on a specific VDSL port.

Syntax

show controllers efm *interface-id* **actual** {**dsrserrs** | **usrserrs** | **txpower** | **rxpower** | **snr** | **link**}

- *interface-id* - ID of the VDSL port.
- **dsrserrs** - Displays the downstream Reed-Solomon errors on the VDSL port.
- **link** - Displays the VDSL link status of the VDSL port.
- **rxpower** - Displays the local receive power (dBm/Hz) on the remote customer premises equipment (CPE) port.
- **snr** - Displays the signal-to-noise ratio (SNR) ratio on the VDSL port.
- **txpower** - Displays the remote transmit power (dBm/Hz) on the VDSL port.
- **usrserrs** - Displays the upstream Reed-Solomon errors on the VDSL port.

Default Setting

None

Command Mode

Privileged EXEC

Command Usage

SNR and Reed-Solomon error information display the quality of the VDSL link.

- The SNR represents the upper limit of received signal to noise ratio that the switch will handle before disconnecting from the remote CPE.
- The Reed-Solomon errors show the number of errors detected and corrected in the data being received on, and transmitted from, the VDSL ports. Reed-Solomon errors are the result of noise exceeding the noise margin.

Example

The following example displays the current values of the VDSL link on VDSL switch port 2.

```
Console#show controller efm Ethernet 1/2 actual dsrserrs
 Downstream Reed-Solomon errors: 0
Console#show controller efm Ethernet 1/2 actual link
 Link status: Down
Console#show controller efm Ethernet 1/2 actual rxpower
 Local receive power: 26.00 dBm/Hz
Console#show controller efm Ethernet 1/2 actual snr
 SNR: 27.00 dB
Console#show controller efm Ethernet 1/2 actual txpower
 Remote transmit power: -89.70 dBm/Hz
Console#show controller efm Ethernet 1/2 actual usrserrs
 Upstream Reed-Solomon errors: 0
Console#
```

Related Commands

show controllers efm admin (4-114)
show controllers efm profile (4-114)

show controllers efm admin

Use this command to display the actual values of the VDSL link on a specific VDSL port.

Syntax

show controllers efm *interface-id* **admin** {**dsrate** | **usrate**}

- *interface-id* - ID of the VDSL port.
- **dsrate** - Displays the downstream rate (Mbps) of the VDSL link.
- **usrate** - Displays the upstream rate (Mbps) of the VDSL link.

Default Setting

None

Command Mode

Privileged EXEC

Command Usage

This command displays the profile settings of a VDSL port. This profile determines the upstream and downstream rates.

Example

```
Console#show controller efm Ethernet 1/1 admin usrate
 Upstream rate: 12.50 Mbps
Console#show controller efm Ethernet 1/1 admin dsrate
 Downstream rate: 12.50 Mbps
Console#
```

Related Commands

show controllers efm actual (4-113)
show controllers efm profile (4-114)

show controllers efm profile

Use this command to to display information about the profiles available on the switch, and how they are assigned to the VDSL ports.

Syntax

show controllers efm profile {**mapping** | **names**}

- **mapping** - Displays a list of the VDSL ports and their assigned profiles.
- **names** - Displays the names, types, and upstream and downstream data rates of all profiles available on the switch. Overall data rates are displayed The usable data rates are somewhat lower.

Default Setting

None

Command Mode

Privileged EXEC

Command Usage

See **efm profile global** (4-103) for the VDSL profiles shipped with the switch, and for the their upstream and downstream data rates.

Examples

This example shows sample output from the **show controllers efm profile mapping** command**.**

```
Console#show controllers efm profile mapping
Interface        Port Profile           Status
-------------    --------------------   --------
Ethernet 1/1     Default                Active
Ethernet 1/2     S1-16-16               Active
Ethernet 1/3     Default                Active
Ethernet 1/4     Default                Active
Ethernet 1/5     Default                Active
Ethernet 1/6     Default                Active
Ethernet 1/7     Default                Active
Ethernet 1/8     Default                Active
Ethernet 1/9     Default                Active
Ethernet 1/10    Default                Active
Ethernet 1/11    Default                Active
Ethernet 1/12    Default                Active
Console#
```

This example shows sample output from the **show controllers efm profile names** command**.**

```
Console#show controllers efm profile names
Profile Name           Type      Downstream Rate(Mbps)   Upstream Rate(Mbps)
--------------------   -------   ---------------------   ---------------------
Default                Public    1.20                    1.40
A1-02OAG-R1            Public    7.56                    2.43
A2-02OAG-R1            Public    10.80                   2.43
A3-01OAG-R1            Public    17.28                   3.78
A4-01OAG-R1            Public    25.92                   4.72
S1-03OAG-R1            Public    7.56                    7.56
S2-03OAG-R1            Public    10.80                   10.40
S3-00OAG-R1            Public    17.28                   16.47
S1-16-16               Private   16.74                   16.20
S2-16-16A              Private   16.74                   16.20
A1-34-11               Private   33.75                   11.34
A2-34-11A              Private   33.75                   11.34
A3-25-3                Private   25.38                   3.24
A4-45-5                Private   44.55                   5.13
A5-50-7                Private   50.49                   7.29
A6-22-3A               Private   22.55                   3.24
A7-40-5A               Private   40.91                   5.13
A8-46-7A               Private   46.44                   7.29
TLAN                   Private   17.01                   5.40
Max-Rate               Private   71.28                   40.50
Console#
```

Related Commands

show controllers efm actual (4-113)
show controllers efm admin (4-114)

show controllers efm status

Use this command to display the VDSL link statistics and profile information on a specific VDSL port including link state, link duration, data rates, power levels, signal-to-noise ratio, and Reed-Solomon errors.

Syntax

show controllers efm status {**link** | **profile**} *interface-id*

- **interface** - id - ID of the VDSL port
- **link** - Displays VDSL link parameters and status.
- **profile** - Displays VDSL link parameters and status.

Default Setting

None

Command Mode

Privileged EXEC

Command Usage

SNR and Reed-Solomon error information display the quality of the VDSL link.

- The SNR represents the upper limit of received signal to noise ratio that the switch will handle before disconnecting from the remote CPE.
- The Reed-Solomon errors show the number of errors detected and corrected in the data being received on and transmitted from the VDSL ports. Reed-Solomon errors are the result of noise exceeding the noise margin.

  Note: The Reed-Solomon errors are reset each time the **show controllers efm status link** command is performed.
- Interleaving improves Reed Solomon error correction when there is pulse noise. A greater degree of interleaving will provide more protection against pulse noise but will increase transmission delay and reduce the effective bandwidth of the link. The degree of interleaving can be increased by increasing M or I. M is the interleaving depth indes and I is the interleaving block length. For details see “VDSL Port Link Status” on page 3-60
- If PBO is enabled the power of transmission from the port will automatically be adjusted to ensure that the signal successfully reaches the reception port.

Examples

This example shows sample output from the **show controllers efm status link** command

```
Console#show controllers efm status link Ethernet 1/1
Interface      Link       SNR (dB)         RS Errs        Interleaver
                       DS1  DS2  US1  US2             DS.M DS.I US.M US.I PBO
-------------  ----  --------------------  --------  ------------------ ---
Ethernet 1/1   Up     45.0 35.0 46.0 44.0  0           16    8    8    8  on
Console#
```

This example shows sample output from the **show controllers efm status profile** command

```
Interface      Link  Uptime    Profile Name          DSRate  USRate  Fail
-------------  ----  --------  --------------------  ------  ------  ----
Ethernet 1/1   Up     0:38:30  default               4.17    1.56    0
Ethernet 1/2   Down   0: 0: 0  default               0.00    0.00    0
Ethernet 1/3   Down   0: 0: 0  default               0.00    0.00    0
Ethernet 1/4   Down   0: 0: 0  default               0.00    0.00    0
Ethernet 1/5   Down   0: 0: 0  default               0.00    0.00    0
Ethernet 1/6   Down   0: 0: 0  default               0.00    0.00    0
Ethernet 1/7   Down   0: 0: 0  default               0.00    0.00    0
Ethernet 1/8   Down   0: 0: 0  default               0.00    0.00    0
```

Related Commands

show controllers efm interface-id actual
show controllers efm interface-id admin

show controllers efm remote ethernet mode

Use this command to display the connected CPE ethernet mode.

Syntax

show controllers efm remote ethernet mode *interface-id*

interface-id – ID of the VDSL port.

Default Setting

None

Command Mode

Privileged EXEC

Command Usage

To obtain the Ethernet mode from the CPE side VDSL chip

Examples

```
Console#show controllers efm remote ethernet mode ethernet 1/1
Interface        Speed         Duplex
-------------    ----------    --------
Ethernet 1/1     100             Full
Console#
```

Related Commands

show controllers efm actual (4-113)
show controllers efm admin (4-114)
show controllers efm status (4-116)
show controllers efm channel-performance (4-119)

show controllers efm-noise-margin

This command displays the noise margin for the selected port.

Syntax

show controllers efm noise-margin

Default Setting

Default: 0 dBm

Command Mode

Privileged EXEC

Command Usage

The noise margin indicates how much the noise on the specific VDSL port can increase before the signal is affected. As the noise on the line increases, the margin will approach zero. If the noise exceeds the current noise margin, the signal will be lost. You will then need to increase the margin until the signal is restored. Range: 0-9 dBm.

Examples

```
Console#show controllers efm noise-margin
Interface        Noise Margin
                 DS  US
--------------   -------------
Ethernet 1/1     0  0
Ethernet 1/2     0  0
Ethernet 1/3     0  0
Ethernet 1/4     0  0
Ethernet 1/5     0  0
Ethernet 1/6     0  0
Ethernet 1/7     0  0
Ethernet 1/8     0  0
Ethernet 1/9     0  0
Ethernet 1/10    0  0
Ethernet 1/11    0  0
Ethernet 1/12    0  0
Ethernet 1/13    0  0
Ethernet 1/14    0  0
Console#
```

Related Commands

show controllers efm actual (4-113)
show controllers efm admin (4-114)
show controllers efm status (4-116)
show controllers efm channel-performance (4-119)

show controllers efm channel-performance

This command display the channel performance for the channels in a VDSL line. For details see “VDSL Performance Monitor Information” on page 3-66.

Syntax

show controllers efm channel-performance {**vtu-r** | **vtu-c**} [**fast** | **slow**] [*interface*] [{**15-minutes** | **1-day**} [*interval*]]

- **vtu-r** – VTU (VDSL Transceiver Unit) at the remote end of the line
- **vtu-r** – VTU Transceiver at the near (central) end of the line
- **fast** – Fast channel
- **slow** – slow channel
- *interface* – Ethernet interface to display
  - *unit/port*
    - *unit* - This is device 1
    - *port* - Port number
- **15-minutes** – Performance at intervals of 15 minutes
- **1-day** – Performance at intervals of 1 day
- *interval* – Number of intervals to show, starting at the latest interval. If this is omitted, all intervals are shown.

Command Mode

Privileged EXEC

Examples

```
Console#show controllers efm channel-performance vtu-c fast 1/1 1-day
VDSL_CHAN_1DAY_INTERVAL_ENTRY :

Ethernet 1/1    Channel Interval Number at interval 1 day        0
Ethernet 1/1    Channel Interval monitoring at interval 1 day    0
Ethernet 1/1    Channel Interval Bad Blocks at interval 1 day    0

Console#
```

Related Commands

show controllers efm actual (4-113)
show controllers efm admin (4-114)
show controllers efm status (4-116)

Address Table Commands

These commands are used to configure the address table for filtering specified addresses, displaying current entries, clearing the table, or setting the aging time.

Command	Function	Mode	Page
mac-address-table static	Maps a static address to a port in a VLAN	GC	4-120
clear mac-address-table dynamic	Removes any learned entries from the forwarding database	PE	4-121
show mac-address-table	Displays entries in the bridge-forwarding database	PE	4-121
mac-address-table aging-time	Sets the aging time of the address table	GC	4-122
show mac-address-table aging-time	Shows the aging time for the address table	PE	4-123

mac-address-table static

This command maps a static address to a destination port in a VLAN. Use the **no** form to remove an address.

Syntax

mac-address-table static *mac-address* **interface** *interface* **vlan** *vlan-id* [*action*]
no mac-address-table static *mac-address* **vlan** *vlan-id*

- *mac-address* - MAC address.
- *interface*
  - **ethernet** *unit*/*port*
    - *unit* - This is device 1
    - *port* - Port number
  - **port-channel** *channel-id* (Value: 1)
- *vlan-id* - VLAN ID (Range: 1-4093)
- *action*
  - **delete-on-reset** - Assignment lasts until the switch is reset.
  - **permanent** - Assignment is permanent.

Default Setting

No static addresses are defined. The default mode is permanent.

Command Mode

Global Configuration

Command Usage

The static address for a host device can be assigned to a specific port within a specific VLAN. Use this command to add static addresses to the MAC Address Table. Static addresses have the following characteristics:

- Static addresses will not be removed from the address table when a given interface link is down.

- Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.
- A static address cannot be learned on another port until the address is removed with the **no** form of this command.

Example

```
Console(config)#mac-address-table static 00-e0-29-94-34-de interface
  ethernet 1/1 vlan 1 delete-on-reset
```

clear mac-address-table dynamic

This command removes any learned entries from the forwarding database and clears the transmit and receive counts for any static or system configured entries.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#clear mac-address-table dynamic
```

show mac-address-table

This command shows classes of entries in the bridge-forwarding database.

Syntax

show mac-address-table [**address mac-address** [**mask**]] [**interface** *interface*]
[**vlan** *vlan-id*] [**sort** {**address** | **vlan** | **interface**}]

mac-address **- MAC address.**

- *mask* - Bits to match in the address.
- *interface*
  - **ethernet** *unit*/*port*
    - *unit* - This is device 1.
    - *port* - Port number.
  - **port-channel** *channel-id* (Value: 1)
- *vlan-id* - VLAN ID (Range: 1-4093)
- **sort** - Sort by address, vlan or interface.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- The MAC Address Table contains the MAC addresses associated with each interface. Note that the Type field may include the following types:
  - Learned - Dynamic address entries
  - Permanent - Static entry
  - Delete-on-reset - Static entry to be deleted when system is reset
- The mask should be hexadecimal numbers (representing an equivalent bit mask) in the form xx-xx-xx-xx-xx-xx that is applied to the specified MAC address. Enter hexadecimal numbers, where an equivalent binary bit “0” means to match a bit and “1” means to ignore a bit. For example, a mask of 00-00-00-00-00-00 means an exact match, and a mask of FF-FF-FF-FF-FF-FF means “any.”
- The maximum number of address entries is 8191.

Example

```
Console#show mac-address-table
 Interface Mac Address       Vlan Type
 --------- ----------------- ---- -----------------
  Eth 1/ 1 00-e0-29-94-34-de    1 Delete-on-reset
Console#
```

mac-address-table aging-time

This command sets the aging time for entries in the address table. Use the **no** form to restore the default aging time.

Syntax

mac-address-table aging-time *seconds*
no mac-address-table aging-time

seconds - Aging time. (Range: 10-1000000 seconds; 0 to disable aging)

Default Setting

300 seconds

Command Mode

Global Configuration

Command Usage

The aging time is used to age out dynamically learned forwarding information.

Example

```
Console(config)#mac-address-table aging-time 100
Console(config)#
```

show mac-address-table aging-time

This command shows the aging time for entries in the address table.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show mac-address-table aging-time
 Aging time: 300 sec.
Console#
```

Spanning Tree Commands

This section includes commands that configure the Spanning Tree Algorithm (STA) globally for the switch, and commands that configure STA for the selected interface.

Command	Function	Mode	Page
spanning-tree	Enables the spanning tree protocol	GC	4-124
spanning-tree mode	Configures STP, RSTP mode	GC	4-124
spanning-tree forward-time	Configures the spanning tree bridge forward time	GC	4-125
spanning-tree hello-time	Configures the spanning tree bridge hello time	GC	4-126
spanning-tree max-age	Configures the spanning tree bridge maximum age	GC	4-126
spanning-tree priority	Configures the spanning tree bridge priority	GC	4-127
spanning-tree path-cost method	Configures the path cost method for RSTP	GC	4-128
spanning-tree transmission-limit	Configures the transmission limit for RSTP	GC	4-128
spanning-tree cost	Configures the spanning tree path cost of an interface	IC	4-129
spanning-tree port-priority	Configures the spanning tree priority of an interface	IC	4-130
spanning-tree edge-port	Enables fast forwarding for edge ports	IC	4-130
spanning-tree portfast	Sets an interface to fast forwarding	IC	4-131
spanning-tree link-type	Configures the link type for RSTP	IC	4-132
spanning-tree protocol-migration	Re-checks the appropriate BPDU format	PE	4-133
show spanning-tree	Shows spanning tree configuration for the common spanning tree (i.e., overall bridge), a selected interface, or an instance within the multiple spanning tree	PE	4-133

spanning-tree

This command enables the Spanning Tree Algorithm globally for the switch. Use the **no** form to disable it.

Syntax

[**no**] **spanning-tree**

Default Setting

Spanning tree is enabled.

Command Mode

Global Configuration

Command Usage

The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

Example

This example shows how to enable the Spanning Tree Algorithm for the switch:

```
Console(config)#spanning-tree
Console(config)#
```

spanning-tree mode

This command selects the spanning tree mode for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree mode {**stp** | **rstp**}
no spanning-tree mode

- **stp** - Spanning Tree Protocol (IEEE 802.1D)
- **rstp** - Rapid Spanning Tree Protocol (IEEE 802.1w)

Default Setting

rstp

Command Mode

Global Configuration

Command Usage

- Spanning Tree Protocol
  Uses RSTP for the internal state machine, but sends only 802.1D BPDUs.

- Rapid Spanning Tree Protocol

  RSTP supports connections to either STP or RSTP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:

  - STP Mode – If the switch receives an 802.1D BPDU after a port's migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.
  - RSTP Mode – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.Example

The following example configures the switch to use Rapid Spanning Tree:

```
Console(config)#spanning-tree mode rstp
Console(config)#
```

spanning-tree forward-time

This command configures the spanning tree bridge forward time globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree forward-time *seconds*
no spanning-tree forward-time

seconds - Time in seconds. (Range: 4 - 30 seconds)
The minimum value is the higher of 4 or [(max-age / 2) + 1].

Default Setting

15 seconds

Command Mode

Global Configuration

Command Usage

This command sets the maximum time (in seconds) the root device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to the discarding state; otherwise, temporary data loops might result.

Example

```
Console(config)#spanning-tree forward-time 20
Console(config)#
```

spanning-tree hello-time

This command configures the spanning tree bridge hello time globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree hello-time *time*
no spanning-tree hello-time

time - Time in seconds. (Range: 1-10 seconds).
The maximum value is the lower of 10 or [(max-age / 2) -1].

Default Setting

2 seconds

Command Mode

Global Configuration

Command Usage

This command sets the time interval (in seconds) at which the root device transmits a configuration message.

Example

```
Console(config)#spanning-tree hello-time 5
Console(config)#
```

spanning-tree max-age

This command configures the spanning tree bridge maximum age globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree max-age ***seconds***
no spanning-tree max-age

seconds - Time in seconds. (Range: 6-40 seconds)
The minimum value is the higher of 6 or [2 x (hello-time + 1)].
The maximum value is the lower of 40 or [2 x (forward-time - 1)].

Default Setting

20 seconds

Command Mode

Global Configuration

Command Usage

This command sets the maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network.

Example

```
Console(config)#spanning-tree max-age 40
Console(config)#
```

spanning-tree priority

This command configures the spanning tree priority globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree priority *priority*
no spanning-tree priority

priority - Priority of the bridge. (Range: 0 - 65535)
(Range – 0-61440, in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

Default Setting

32768

Command Mode

Global Configuration

Command Usage

Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.

Example

```
Console(config)#spanning-tree priority 40000
Console(config)#
```

spanning-tree pathcost method

This command configures the path cost method used for Rapid Spanning Tree. Use the **no** form to restore the default.

Syntax

spanning-tree pathcost method {**long** | **short**}
no spanning-tree pathcost method

- **long** - Specifies 32-bit based values that range from 1-200,000,000.
- **short** - Specifies 16-bit based values that range from 1-65535.

Default Setting

Long method

Command Mode

Global Configuration

Command Usage

The path cost method is used to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. Note that path cost (page 4-129) takes precedence over port priority (page 4-130).

Example

```
Console(config)#spanning-tree pathcost method long
Console(config)#
```

spanning-tree transmission-limit

This command configures the minimum interval between the transmission of consecutive RSTP BPDUs. Use the **no** form to restore the default.

Syntax

spanning-tree transmission-limit *count*
no spanning-tree transmission-limit

count - The transmission limit in seconds. (Range: 1-10)

Default Setting

3

Command Mode

Global Configuration

Command Usage

This command limits the maximum transmission rate for BPDUs.

Example

```
Console(config)#spanning-tree transmission-limit 4
Console(config)#
```

spanning-tree cost

This command configures the spanning tree path cost for the specified interface. Use the **no** form to restore the default.

Syntax

spanning-tree cost *cost*
no spanning-tree cost

cost - The path cost for the port. (Range: 1-200,000,000))
The recommended range is:

- Ethernet: 200,000-20,000,000
- Fast Ethernet: 20,000-2,000,000
- Gigabit Ethernet: 2,000-200,000

Default Setting

- Ethernet – half duplex: 2,000,000; full duplex: 1,000,000; trunk: 500,000
- Fast Ethernet – half duplex: 200,000; full duplex: 100,000; trunk: 50,000
- Gigabit Ethernet – full duplex: 10,000; trunk: 5,000

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command is used by the Spanning Tree Algorithm to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media.
- Path cost takes precedence over port priority.
- When the spanning-tree pathcost method (page 4-128) is set to short, the maximum value for path cost is 65,535.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree cost 50
Console(config-if)#
```

spanning-tree port-priority

This command configures the priority for the specified interface. Use the **no** form to restore the default.

Syntax

spanning-tree port-priority *priority*
no spanning-tree port-priority

priority - The priority for a port. (Range: 0-240, in steps of 16)

Default Setting

128

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command defines the priority for the use of a port in the Spanning Tree Algorithm. If the path cost for all ports on a switch are the same, the port with the highest priority (that is, lowest value) will be configured as an active link in the spanning tree.
- Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-priority 0
```

Related Commands

spanning-tree cost (4-129)

spanning-tree edge-port

This command specifies an interface as an edge port. Use the **no** form to restore the default.

Syntax

[**no**] **spanning-tree edge-port**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device.
- This command has the same effect as the **spanning-tree portfast** command.

Example

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#
```

Related Commands

spanning-tree portfast (4-131)

spanning-tree portfast

This command sets an interface to fast forwarding. Use the **no** form to disable fast forwarding.

Syntax

[**no**] **spanning-tree portfast**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command is used to enable/disable the fast spanning-tree mode for the selected port. In this mode, ports skip the Discarding and Learning states, and proceed straight to Forwarding.
- Since end-nodes cannot cause forwarding loops, they can be passed through the spanning tree state changes more quickly than allowed by standard convergence time. Fast forwarding can achieve quicker convergence for end-node workstations and servers, and also overcome other STA related timeout problems. (Remember that fast forwarding should only be enabled for ports connected to a LAN segment that is at the end of a bridged LAN or for an end-node device.)
- This command is the same as **spanning-tree edge-port**, and is only included for backward compatibility with earlier products. Note that this command may be removed for future software versions.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#bridge-group 1 portfast
Console(config-if)#
```

Related Commands

spanning-tree edge-port (4-130)

spanning-tree link-type

This command configures the link type for Rapid Spanning Tree. Use the **no** form to restore the default.

Syntax

spanning-tree link-type {**auto** | **point-to-point** | **shared**}
no spanning-tree link-type

- **auto** - Automatically derived from the duplex mode setting.
- **point-to-point** - Point-to-point link.
- **shared** - Shared medium.

Default Setting

auto

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Specify a point-to-point link if the interface can only be connected to exactly one other bridge, or a shared link if it can be connected to two or more bridges.
- When automatic detection is selected, the switch derives the link type from the duplex mode. A full-duplex interface is considered a point-to-point link, while a half-duplex interface is assumed to be on a shared link.
- RSTP only works on point-to-point links between two bridges. If you designate a port as a shared link, RSTP is forbidden.

Example

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree link-type point-to-point
```

spanning-tree protocol-migration

This command re-checks the appropriate BPDU format to send on the selected interface.

Syntax

spanning-tree protocol-migration *interface*

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Value: 1)

Command Mode

Privileged Exec

Command Usage

If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the spanning-tree protocol-migration command at any time to manually re-check the appropriate BPDU format to send on the selected interfaces (i.e., RSTP or STP-compatible).

Example

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree protocol-migration
Console(config-if)#
```

show spanning-tree

This command shows the configuration for the common spanning tree (CST) or for an instance within the multiple spanning tree (MST).

Syntax

show spanning-tree [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Value: 1)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- Use the **show spanning-tree** command with no parameters to display the spanning tree configuration for the switch and for every interface in the tree.
- Use the **show spanning-tree** *interface* command to display the spanning tree configuration for an interface.
- For a description of the items displayed under “Spanning-tree information,” see “Configuring Global Settings” on page 3-76. For a description of the items displayed for specific interfaces, see “Displaying Interface Settings” on page 3-78.

Example

```
CConsole#show spanning-tree
Spanning-tree information
---------------------------------------------------------------
 Spanning tree mode                :RSTP
 Spanning tree enable/disable      :enable
 Priority                          :32768
 Bridge Hello Time (sec.)          :2
 Bridge Max Age (sec.)             :20
 Bridge Forward Delay (sec.)       :15
 Root Hello Time (sec.)            :2
 Root Max Age (sec.)               :20
 Root Forward Delay (sec.)         :15
 Designated Root                   :32768.000087654321
 Current root port                 :1
 Current root cost                 :200000
 Number of topology changes        :1
 Last topology changes time (sec.):18131
 Transmission limit                :3
 Path Cost Method                  :long
---------------------------------------------------------------
Eth  1/ 1 information
---------------------------------------------------------------
 Admin status          : enable
 Role                  : root
 State                 : forwarding
 Path cost             : 100000
 Priority              : 128
 Designated cost       : 200000
 Designated port       : 128.24
 Designated root       : 32768.0.0000ABCD0000
 Designated bridge     : 32768.0.0030F1552000
 Fast forwarding       : disable
 Forward transitions   : 1
 Admin edge port       : enable
 Oper edge port        : disable
 Admin Link type       : auto
 Oper Link type        : point-to-point
:
Console#
```

VLAN Commands

A VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment. This section describes commands used to create VLAN groups, add port members, specify how VLAN tagging is used, and enable automatic VLAN registration for the selected interface.

Command Groups	Function	Page
Editing VLAN Groups	Sets up VLAN groups, including name, VID and state	4-135
Configuring VLAN Interfaces	Configures VLAN interface parameters, including ingress and egress tagging mode, ingress filtering, and PVID	4-137
Displaying VLAN Information	Displays VLAN groups, status, port members, and MAC addresses	4-141
Configuring Private VLANs	Configures private VLANs, including uplink and downlink ports	4-142

Editing VLAN Groups

Command	Function	Mode	Page
vlan database	Enters VLAN database mode to add, change, and delete VLANs	GC	4-135
vlan	Configures a VLAN, including VID, name and state	VC	4-136

vlan database

This command enters VLAN database mode. All commands in this mode will take effect immediately.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- Use the VLAN database command mode to add, change, and delete VLANs. After finishing configuration changes, you can display the VLAN settings by entering the **show vlan** command.
- Use the **interface vlan** command mode to define the port membership mode and add or remove ports from a VLAN. The results of these commands are written to the running-configuration file, and you can display this file by entering the **show running-config** command.

Example

```
Console(config)#vlan database
Console(config-vlan)#
```

Related Commands

show vlan (4-141)

vlan

This command configures a VLAN. Use the **no** form to restore the default settings or delete a VLAN.

Syntax

vlan *vlan-id* [**name** *vlan-name*] **media ethernet** [**state** {**active** | **suspend**}]
no vlan *vlan-id* [**name** | **state**]

- *vlan-id* - ID of configured VLAN. (Range: 1-4093, no leading zeroes)
- **name** - Keyword to be followed by the VLAN name.
  vlan-name - ASCII string from 1 to 32 characters.
- **media ethernet** - Ethernet media type.
- **state** - Keyword to be followed by the VLAN state.
  - **active** - VLAN is operational.
  - **suspend** - VLAN is suspended. Suspended VLANs do not pass packets.

Default Setting

By default only VLAN 1 exists and is active.

Command Mode

VLAN Database Configuration

Command Usage

- **no vlan** *vlan-id* deletes the VLAN.
- **no vlan** *vlan-id* **name** removes the VLAN name.
- **no vlan** *vlan-id* **state** returns the VLAN to the default state (i.e., active).
- You can configure up to 255 VLANs on the switch.

Example

The following example adds a VLAN, using VLAN ID 105 and name RD5. The VLAN is activated by default.

```
Console(config)#vlan database
Console(config-vlan)#vlan 105 name RD5 media ethernet
Console(config-vlan)#
```

Related Commands

show vlan (4-141)

Configuring VLAN Interfaces

Command	Function	Mode	Page
interface vlan	Enters interface configuration mode for a specified VLAN	IC	4-137
switchport mode	Configures VLAN membership mode for an interface	IC	4-138
switchport acceptable-frame-types	Configures frame types to be accepted by an interface	IC	4-138
switchport ingress-filtering	Enables ingress filtering on an interface	IC	4-139
switchport native vlan	Configures the PVID (native VLAN) of an interface	IC	4-140
switchport allowed vlan	Configures the VLANs associated with an interface	IC	4-140

interface vlan

This command enters interface configuration mode for VLANs, which is used to configure VLAN parameters for a physical interface.

Syntax

interface vlan *vlan-id*

vlan-id - ID of the configured VLAN. (Range: 1-4093, no leading zeroes)

Default Setting

None

Command Mode

Global Configuration

Example

The following example shows how to set the interface configuration mode to VLAN 1, and then assign an IP address to the VLAN:

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.254 255.255.255.0
Console(config-if)#
```

Related Commands

shutdown (4-91)

switchport mode

This command configures the VLAN membership mode for a port. Use the **no** form to restore the default.

Syntax

switchport mode {**trunk** | **hybrid**}
no switchport mode

- **trunk** - Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. However, note that frames belonging to the port's default VLAN (i.e., associated with the PVID) are sent untagged.
- **hybrid** - Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.

Default Setting

All ports are in hybrid mode with the PVID set to VLAN 1.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

The following shows how to set the configuration mode to port 1, and then set the switchport mode to hybrid:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport mode hybrid
Console(config-if)#
```

Related Commands

switchport acceptable-frame-types (4-138)

switchport acceptable-frame-types

This command configures the acceptable frame types for a port. Use the **no** form to restore the default.

Syntax

switchport acceptable-frame-types {**all** | **tagged**}
no switchport acceptable-frame-types

- **all** - The port accepts all frames, tagged or untagged.
- **tagged** - The port only receives tagged frames.

Default Setting

All frame types

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN.

Example

The following example shows how to restrict the traffic received on port 1 to tagged frames:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#
```

Related Commands

switchport mode (4-138)

switchport ingress-filtering

This command enables ingress filtering for an interface. Use the **no** form to restore the default.

Syntax

[**no**] **switchport ingress-filtering**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Ingress filtering only affects tagged frames.
- If ingress filtering is disabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be flooded to all other ports (except for those VLANs explicitly forbidden on this port).
- If ingress filtering is enabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be discarded.
- Ingress filtering does not affect VLAN independent BPDU frames, such STA. However, they do affect VLAN dependent BPDU frames, such as GMRP.

Example

The following example shows how to set the interface to port 1 and then enable ingress filtering:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport ingress-filtering
Console(config-if)#
```

switchport native vlan

This command configures the PVID (i.e., default VLAN ID) for a port. Use the **no** form to restore the default.

Syntax

switchport native vlan *vlan-id*
no switchport native vlan

vlan-id - Default VLAN ID for a port. (Range: 1-4093, no leading zeroes)

Default Setting

VLAN 1

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- If an interface is not a member of VLAN 1 and you assign its PVID to this VLAN, the interface will automatically be added to VLAN 1 as an untagged member. For all other VLANs, an interface must first be configured as an untagged member before you can assign its PVID to that group.
- If acceptable frame types is set to **all** or switchport mode is set to **hybrid**, the PVID will be inserted into all untagged frames entering the ingress port.

Example

The following example shows how to set the PVID for port 1 to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport native vlan 3
Console(config-if)#
```

switchport allowed vlan

This command configures VLAN groups on the selected interface. Use the **no** form to restore the default.

Syntax

switchport allowed vlan {**add** *vlan-list* [**tagged** | **untagged**] | **remove** *vlan-list*}
no switchport allowed vlan

- **add** *vlan-list* - List of VLAN identifiers to add.
- **remove** *vlan-list* - List of VLAN identifiers to remove.
- *vlan-list* - Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. Do not enter leading zeros. (Range: 1-4093).

Default Setting

All ports are assigned to VLAN 1 by default.
The default frame type is untagged.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- A port, or a trunk with switchport mode set to **hybrid**, must be assigned to at least one VLAN as untagged.
- If a trunk has switchport mode set to **trunk** (i.e., 1Q Trunk), then you can only assign an interface to VLAN groups as a tagged member.
- Frames are always tagged within the switch. The tagged/untagged parameter used when adding a VLAN to an interface tells the switch whether to keep or remove the tag from a frame on egress.
- If none of the intermediate network devices nor the host at the other end of the connection supports VLANs, the interface should be added to these VLANs as an untagged member. Otherwise, it is only necessary to add at most one VLAN as untagged, and this should correspond to the native VLAN for the interface.
- If a VLAN on the forbidden list for an interface is manually added to that interface, the VLAN is automatically removed from the forbidden list for that interface.

Example

The following example shows how to add VLANs 1, 2, 5 and 6 to the allowed list as tagged VLANs for port 1:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport allowed vlan add 1,2,5,6 tagged
Console(config-if)#
```

Displaying VLAN Information

Command	Function	Mode	Page
show vlan	Shows VLAN information	NE, PE	4-141
show interfaces status vlan	Displays status for the specified VLAN interface	NE, PE	4-93
show interfaces switchport	Displays the administrative and operational status of an interface	NE, PE	4-95

show vlan

This command shows VLAN information.

Syntax

show vlan [**id** *vlan-id* | **name** *vlan-name*]

- **id** - Keyword to be followed by the VLAN ID.
  vlan-id - ID of the configured VLAN. (Range: 1-4094, no leading zeroes)
- **name** - Keyword to be followed by the VLAN name.
  vlan-name - ASCII string from 1 to 32 characters.

Default Setting

Shows all VLANs.

Command Mode

Normal Exec, Privileged Exec

Example

The following example shows how to display information for VLAN 1:

```
Console#show vlan id 1
VLAN Type    Name             Status    Ports/Channel groups
---- ------- ---------------- --------- ----------------------------------
   1  Static      DefaultVlan    Active Eth1/ 1 Eth1/ 2 Eth1/ 3 Eth1/ 4 Eth1/ 5
                                        Eth1/ 6 Eth1/ 7 Eth1/ 8 Eth1/ 9 Eth1/10
                                        Eth1/11 Eth1/12 Eth1/13 Eth1/14 Eth1/15
                                        Eth1/16 Eth1/17 Eth1/18 Eth1/19 Eth1/20
                                        Eth1/21 Eth1/22 Eth1/23 Eth1/24
Console#
```

Configuring Private VLANs

pvlan

Use this command in global configuration mode to enable or configure private VLAN. Use the no form of this command to disable it.

Command	Function	Mode	Page
pvlan	Enables Private VLAN globally for the switch	GC	4-142
pvlan up-link down-link	Configures uplink and downlink ports	GC	4-142
show pvlan	shows the private VLAN configuration settings on this switch	PE	4-143

Syntax

pvlan
pvlan up-link *interface-list* **down-link** *interface-list*
no pvlan

- **up-link** – Specifies a list of uplink interfaces.
- **down-link** – Specifies a list of downlink interfaces.

Default Setting

No pvlan

Command Mode

Global configuration

Command Usage

A Private VLAN allows modification of the default VLAN to provide port-based security and isolation between ports within the VLAN. Data traffic on the downlink ports can only be forwarded to, and from, the uplink port. Private VLANs and normal VLANs can exist simultaneously within the same switch.

Example

This example globally enables private vlan, and then configures ports 13 and 14 as uplink ports, and ports 1-8 as downlink ports.

```
Console(config)#pvlan
Console(config)#Console(config)#pvlan up-link ethernet 1/13-14 down-link
ethernet 1/1-8
Console(config)#end
Console#
```

show pvlan

Use this command to show the private VLAN configuration settings on this switch.

Syntax

show pvlan

Default Setting

None

Command Mode

Privileged Executive

Example

```
Console#show pvlan
Private VLAN status: Enabled
Up-link port:
 Ethernet 1/13
 Ethernet 1/14
Down-link port:
 Ethernet 1/1
 Ethernet 1/2
 Ethernet 1/3
 Ethernet 1/4
 Ethernet 1/5
 Ethernet 1/6
 Ethernet 1/7
 Ethernet 1/8
Console#
```

Bridge Extension Commands

This section describes how to display default configuration settings for the Bridge Extension MIB.

Command	Function	Mode	Page
show bridge-ext	Shows the global bridge extension configuration	PE	4-144

show bridge-ext

This command shows the configuration for bridge extension commands.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

See “Displaying Basic VLAN Information” on page 3-85 and “Displaying Bridge Extension Capabilities” on page 3-10 for a description of the displayed items.

Example

```
Console#show bridge-ext
 Max support vlan numbers: 255
 Max support vlan ID: 4093
 Extended multicast filtering services: No
 Static entry individual port: Yes
 VLAN learning: IVL
 Configurable PVID tagging: Yes
 Local VLAN capable: No
 Traffic classes: Enabled
 GMRP: Disabled
Console#
```

Priority Commands

The commands described in this section allow you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with four priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. You can set the default priority for each interface, the relative weight of each queue, and the mapping of frame priority tags to the switch's priority queues.

Command Groups	Function	Page
Priority (Layer 2)	Configures default priority for untagged frames, sets queue weights, and maps class of service tags to hardware queues	4-145
Priority (Layer 3 and 4)	Maps TCP ports, IP precedence tags, or IP DSCP tags to class of service values	4-150

Priority Commands (Layer 2)

Command	Function	Mode	Page
switchport priority default	Sets a port priority for incoming untagged frames	IC	4-145
queue mode	Sets the queue mode to strict priority or Weighted Round-Robin (WRR)	GC	4-146
queue bandwidth	Assigns round-robin weights to the priority queues	GC	4-147
queue cos map	Assigns class-of-service values to the priority queues	IC	4-148
show queue mode	Shows the current queue mode	PE	4-149
show queue bandwidth	Shows round-robin weights assigned to the priority queues	PE	4-149
show queue cos-map	Shows the class-of-service map	PE	4-149
show interfaces switchport	Displays the administrative and operational status of an interface	PE	4-95

switchport priority default

This command sets a priority for incoming untagged frames. Use the **no** form to restore the default value.

Syntax

switchport priority default *default-priority-id*
no switchport priority default

default-priority-id - The priority number for untagged ingress traffic. The priority is a number from 0 to 7. Seven is the highest priority.

Default Setting

The priority is not set, and the default value for untagged frames received on the interface is zero.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- The default priority applies for an untagged frame received on a port set to accept all frame types (i.e, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.
- This switch provides four priority queues for each port. It is configured to use Weighted Round Robin, which can be viewed with the **show queue bandwidth** command. Inbound frames that do not have VLAN tags are tagged with the input port's default ingress user priority, and then placed in the appropriate priority queue at the output port. The default priority for all ingress ports is zero. Therefore, any inbound frames that do not have priority tags will be placed in queue 0 of the output port. (Note that if the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.)

Example

The following example shows how to set a default priority on port 3 to 5:

```
Console(config)#interface ethernet 1/3
Console(config-if)#interface ethernet 1/3
```

queue mode

This command sets the queue mode to strict priority or Weighted Round-Robin (WRR) for the class of service (CoS) priority queues. Use the **no** form to restore the default value.

Syntax

queue mode {strict | **wrr**}
no queue mode

- **strict** - Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues.
- **wrr** - Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights 1, 3, 5, 7 for queues 0 - 3 respectively.

Default Setting

Weighted Round Robin

Command Mode

Global Configuration

Command Usage

You can set the switch to service the queues based on a strict rule that requires all traffic in a higher priority queue to be processed before lower priority queues are serviced, or use Weighted Round-Robin (WRR) queuing that specifies a relative weight of each queue. WRR uses a predefined relative weight for each queue that determines the percentage of service time the switch services each queue before moving on to the next queue. This prevents the head-of-line blocking that can occur with strict priority queuing.

Example

The following example sets the queue mode to strict priority service mode:

```
Console(config)#queue mode strict
Console(config)#
```

queue bandwidth

This command assigns weighted round-robin (WRR) weights to the four class of service (CoS) priority queues. Use the **no** form to restore the default weights.

Syntax

queue bandwidth *weight1...weight4*
no queue bandwidth

weight1...weight4 - The ratio of weights for queues 0 - 3 determines the weights used by the WRR scheduler. (Range: 1 - 15)

Default Setting

Weights 1, 4, 16, 64 are assigned to queues 0 - 3 respectively.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

WRR controls bandwidth sharing at the egress port by defining scheduling weights.

Example

This example shows how to assign WRR weights to each of the priority queues:

```
Console(config)#queue bandwidth 1 3 5 7
Console(config)#
```

Related Commands

show queue bandwidth (4-149)

queue cos-map

This command assigns class of service (CoS) values to the priority queues (i.e., hardware output queues 0 - 3). Use the **no** form set the CoS map to the default values.

Syntax

queue cos-map *queue_id* [*cos1 ... cosn*]
no queue cos-map

- *queue_id* - The ID of the priority queue.
- Ranges are 0 to 4, where 4 is the highest priority queue.
- *cos1 .. cosn* - The CoS values that are mapped to the queue ID. It is a space-separated list of numbers. The CoS value is a number from 0 to 7, where 7 is the highest priority.

Default Setting

This switch supports Class of Service by using four priority queues, with Weighted Round Robin queuing for each port. Eight separate traffic classes are defined in IEEE 802.1p. The default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown below.

Queue	0	1	2	3
Priority	1, 2	0, 3	4, 5	6, 7

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- CoS values assigned at the ingress port are also used at the egress port.
- This command sets the CoS priority for all interfaces.

Example

The following example shows how to change the CoS assignments to a one-to-one mapping:

```
Console(config)#interface ethernet 1/1
Console(config-if)#queue cos-map 0 0
Console(config-if)#queue cos-map 1 1
Console(config-if)#queue cos-map 2 2
Console(config-if)#exit
Console#show queue cos-map ethernet 1/1
Information of Eth 1/1
 Traffic Class : 0 1 2 3 4 5 6 7
 Priority Queue: 0 1 2 1 2 2 3 3
```

Related Commands

show queue cos-map (4-149)

show queue mode

This command shows the current queue mode.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#sh queue mode

Wrr status: Enabled
Console#
```

show queue bandwidth

This command displays the weighted round-robin (WRR) bandwidth allocation for the eight priority queues.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show queue bandwidth
 Queue ID  Weight
 --------  ------
    0        1
    1        3
    2        5
    3        7
Console#
```

show queue cos-map

This command shows the class of service priority map.

Syntax

show queue cos-map *interface*

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Value: 1)

Default Setting

None

Command Mode

Privileged Exec

Example

```
onsole#show queue cos-map ethernet 1/1
Information of Eth 1/1
 Traffic Class : 0 1 2 3 4 5 6 7
 Priority Queue: 0 0 0 1 1 2 3 2
Console#
```

Priority Commands (Layer 3 and 4)

Command	Function	Mode	Page
map ip precedence	Enables IP precedence class of service mapping	GC	4-150
map ip precedence	Maps IP precedence value to a class of service	IC	4-151
map ip dscp	Enables IP DSCP class of service mapping	GC	4-151
map ip dscp	Maps IP DSCP value to a class of service	IC	4-152
show map ip precedence	Shows the IP precedence map	PE	4-154
show map ip dscp	Shows the IP DSCP map	PE	4-154

map ip precedence (Global Configuration)

This command enables IP precedence mapping (i.e., IP Type of Service). Use the **no** form to disable IP precedence mapping.

Syntax

[no] map ip precedence

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- IP Precedence and IP DSCP cannot both be enabled. Enabling one of these priority types will automatically disable the other type.

Example

The following example shows how to enable IP precedence mapping globally:

```
Console(config)#map ip precedence
Console(config)#
```

map ip precedence (Interface Configuration)

This command sets IP precedence priority (i.e., IP Type of Service priority). Use the **no** form to restore the default table.

Syntax

map ip precedence *ip-precedence-value* **cos** *cos-value*
no map ip precedence

- *precedence-value* - 3-bit precedence value. (Range: 0-7)
- *cos-value* - Class-of-Service value (Range: 0-7)

Default Setting

The list below shows the default priority mapping.

IP Precedence Value	0	1	2	3	4	5	6	7
CoS Value	0	1	2	3	4	5	6	7

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- IP Precedence values are mapped to default Class of Service values on a one-to-one basis according to recommendations in the IEEE 802.1p standard, and then subsequently mapped to the eight hardware priority queues.
- This command sets the IP Precedence for all interfaces.

Example

The following example shows how to map IP precedence value 1 to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip precedence 1 cos 0
Console(config-if)#
```

map ip dscp (Global Configuration)

This command enables IP DSCP mapping (i.e., Differentiated Services Code Point mapping). Use the **no** form to disable IP DSCP mapping.

Syntax

[**no**] **map ip dscp**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- IP Precedence and IP DSCP cannot both be enabled. Enabling one of these priority types will automatically disable the other type.

Example

The following example shows how to enable IP DSCP mapping globally:

```
Console(config)#map ip dscp
Console(config)#
```

map ip dscp (Interface Configuration)

This command sets IP DSCP priority (i.e., Differentiated Services Code Point priority). Use the **no** form to restore the default table.

Syntax

map ip dscp *dscp-value* cos *cos-value*
no map ip dscp

- *dscp-value* - 8-bit DSCP value. (Range: 0-255)
- *cos-value* - Class-of-Service value (Range: 0-7)

Default Setting

The DSCP default values are defined in the following table. Note that all the DSCP values that are not specified are mapped to CoS value 0.

IP DSCP Value	CoS Value
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4
38, 40, 42	5
48	6
46, 56	7

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.

- DSCP priority values are mapped to default Class of Service values according to recommendations in the IEEE 802.1p standard, and then subsequently mapped to the eight hardware priority queues.
- This command sets the IP DSCP priority for all interfaces.

Example

The following example shows how to map IP DSCP value 1 to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip dscp 1 cos 0
Console(config-if)#
```

map ip port (Global Configuration)

Use this command to enable IP port mapping (i.e., class of service mapping for TCP/UDP sockets). Use the **no** form to disable IP port mapping.

Syntax

map ip port
no map ip port

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.

Example

The following example shows how to enable TCP/UDP port mapping globally:

```
Console(config)#map ip port
Console(config)#
```

map ip port (Interface Configuration)

Use this command to set IP port priority (i.e., TCP/UDP port priority). Use the **no** form to remove a specific setting.

Syntax

map ip port *port-number* **cos** *cos-value*
no map ip port *port-number*

- *port-number* - 16-bit TCP/UDP port number. (Range: 0-65535)
- *cos-value* - Class-of-Service value (Range: 0-7)

Default Setting

None

show map ip precedence

This command shows the IP precedence priority map.

Syntax

show map ip precedence *interface*

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Value: 1)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show map ip precedence ethernet 1/5
Precedence mapping status: disabled

 Port      Precedence COS
 --------- ---------- ---
  Eth 1/ 5          0   0
  Eth 1/ 5          1   1
  Eth 1/ 5          2   2
  Eth 1/ 5          3   3
  Eth 1/ 5          4   4
  Eth 1/ 5          5   5
  Eth 1/ 5          6   6
  Eth 1/ 5          7   7
Console#
```

Related Commands

map ip precedence (Global Configuration) (4-150)
map ip precedence (Interface Configuration) (4-151)

show map ip dscp

This command shows the IP DSCP priority map.

Syntax

show map ip dscp *interface*

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Value: 1)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show map ip dscp ethernet 1/1
DSCP mapping status: disabled

 Port      DSCP COS
 --------- ---- ---
  Eth 1/ 1    0   0
  Eth 1/ 1    1   0
  Eth 1/ 1    2   0
  Eth 1/ 1    3   0
⋮
  Eth 1/ 1   61   0
  Eth 1/ 1   62   0
  Eth 1/ 1   63   0
Console#
```

Related Commands

map ip dscp (Global Configuration) (4-151)
map ip dscp (Interface Configuration) (4-152)

show map ip port

Use this command to show the IP port priority map.

Syntax

show map ip port [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** *channel-id* (Range: 1-6)

Default Setting

None

Command Mode

Privileged Exec

Example

The following shows that HTTP traffic has been mapped to CoS value 0:

```
Console#show map ip port
TCP port mapping status: disabled

 Port      Port no. COS
 --------- -------- ---
  Eth 1/ 5       80   0
Console#
```

Related Commands

map ip port (Interface Configuration) (4-153)

Multicast Filtering Commands

This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts that want to receive a specific multicast service. It identifies the ports containing hosts requesting a service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service.

Command Groups	Function	Page
IGMP Snooping	Configures multicast groups via IGMP snooping or static assignment, sets the IGMP version, displays current snooping and query settings, and displays the multicast service and group members	4-156
IGMP Query	Configures IGMP query parameters for multicast filtering at Layer 2	4-159
Static Multicast Routing	Configures static multicast router ports	4-163

IGMP Snooping Commands

Command	Function	Mode	Page
ip igmp snooping	Enables IGMP snooping	GC	4-156
ip igmp snooping vlan static	Adds an interface as a member of a multicast group	GC	4-157
ip igmp snooping version	Configures the IGMP version for snooping	GC	4-157
show ip igmp snooping	Shows the IGMP snooping and query configuration	PE	4-158
show mac-address-table multicast	Shows the IGMP snooping MAC multicast list	PE	4-159

ip igmp snooping

This command enables IGMP snooping on this switch. Use the **no** form to disable it.

Syntax

[no] ip igmp snooping

Default Setting

Enabled

Command Mode

Global Configuration

Example

The following example enables IGMP snooping.

```
Console(config)#ip igmp snooping
Console(config)#
```

ip igmp snooping vlan static

This command adds a port to a multicast group. Use the **no** form to remove the port.

Syntax

[**no**] **ip igmp snooping vlan** *vlan-id* **static** *ip-address interface*

- *vlan-id* - VLAN ID (Range: 1-4093)
- *ip-address* - IP address for multicast group
- *interface*
  - **ethernet** *unit*/*port*
    - *unit* - This is device 1.
    - *port* - Port number.
  - **port-channel** *channel-id* (Value: 1)

Default Setting

None

Command Mode

Global Configuration

Example

The following shows how to statically configure a multicast group on a port:

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12 ethernet 1/5
Console(config)#
```

ip igmp snooping version

This command configures the IGMP snooping version. Use the **no** form to restore the default.

Syntax

ip igmp snooping version {**1** | **2**}
no ip igmp snooping version

- **1** - IGMP Version 1
- **2** - IGMP Version 2

Default Setting

IGMP Version 2

Command Mode

Global Configuration

Command Usage

All systems on the subnet must support the same version. If there are legacy devices in your network that only support Version 1, you will also have to configure this switch to use Version 1.
Some commands are only enabled for IGMPv2, including **ip igmp query-max-response-time** and **ip igmp query-timeout**.

Example

The following configures the switch to use IGMP Version 1:

```
Console(config)#ip igmp snooping version 1
Console(config)#
```

show ip igmp snooping

This command shows the IGMP snooping configuration.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

See “Configuring IGMP Snooping and Query Parameters” on page 3-107 for a description of the displayed items.

Example

The following shows the current IGMP snooping configuration:

```
Console#show ip igmp snooping
 Service status: Enabled
 Querier status: Enabled
 Query count: 2
 Query interval: 125 sec
 Query max response time: 10 sec
 Router port expire time: 300 sec
 IGMP snooping version: Version 2
Console#
```

show mac-address-table multicast

This command shows known multicast addresses.

Syntax

show mac-address-table multicast [**vlan** ***vlan-id***] [**user** | **igmp-snooping**]

- *vlan-id* - VLAN ID (1 to 4094)
- **user** - Display only the user-configured multicast entries.
- **igmp-snooping** - Display only entries learned through IGMP snooping.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Member types displayed include IGMP or USER, depending on selected options.

Example

The following shows the multicast entries learned through IGMP snooping for VLAN 1:

```
Console#show mac-address-table multicast vlan 1 igmp-snooping
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1       224.1.2.3      Eth1/11    IGMP
Console#
```

IGMP Query Commands (Layer 2)

Command	Function	Mode	Page
ip igmp snooping querier	Allows this device to act as the querier for IGMP snooping	GC	4-160
ip igmp snooping query-count	Configures the query count	GC	4-160
ip igmp snooping query-interval	Configures the query interval	GC	4-161
ip igmp snooping query-max-response-time	Configures the report delay	GC	4-161
ip igmp snooping router-port-expire-time	Configures the query timeout	GC	4-162

ip igmp snooping querier

This command enables the switch as an IGMP querier. Use the **no** form to disable it.

Syntax

[**no**] **ip igmp snooping querier**

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

If enabled, the switch will serve as querier if elected. The querier is responsible for asking hosts if they want to receive multicast traffic.

Example

```
Console(config)#ip igmp snooping querier
Console(config)#
```

ip igmp snooping query-count

This command configures the query count. Use the **no** form to restore the default.

Syntax

ip igmp snooping query-count *count*
no ip igmp snooping query-count

count - The maximum number of queries issued for which there has been no response before the switch takes action to drop a client from the multicast group. (Range: 2-10)

Default Setting

2 times

Command Mode

Global Configuration

Command Usage

The query count defines how long the querier waits for a response from a multicast client before taking action. If a querier has sent a number of queries defined by this command, but a client has not responded, a countdown timer is started using the time defined by ip igmp snooping query-max-response-time. If the countdown finishes, and the client still has not responded, then that client is considered to have left the multicast group.

Example

The following shows how to configure the query count to 10:

```
Console(config)#ip igmp snooping query-count 10
Console(config)#
```

Related Commands

ip igmp snooping query-max-response-time (4-161)

ip igmp snooping query-interval

This command configures the query interval. Use the **no** form to restore the default.

Syntax

ip igmp snooping query-interval *seconds*
no ip igmp snooping query-interval

seconds - The frequency at which the switch sends IGMP host-query messages. (Range: 60-125)

Default Setting

125 seconds

Command Mode

Global Configuration

Example

The following shows how to configure the query interval to 100 seconds:

```
Console(config)#ip igmp snooping query-interval 100
Console(config)#
```

ip igmp snooping query-max-response-time

This command configures the query report delay. Use the **no** form to restore the default.

Syntax

ip igmp snooping query-max-response-time *seconds*
no ip igmp snooping query-max-response-time

seconds - The report delay advertised in IGMP queries. (Range: 5-30)

Default Setting

10 seconds

Command Mode

Global Configuration

Command Usage

- The switch must be using IGMPv2 for this command to take effect.
- This command defines the time after a query, during which a response is expected from a multicast client. If a querier has sent a number of queries defined by the **ip igmp snooping query-count**, but a client has not responded, a countdown timer is started using an initial value set by this command. If the countdown finishes, and the client still has not responded, then that client is considered to have left the multicast group.

Example

The following shows how to configure the maximum response time to 20 seconds:

```
Console(config)#ip igmp snooping query-max-response-time 20
Console(config)#
```

Related Commands

ip igmp snooping version (4-157)
ip igmp snooping query-max-response-time (4-161)

ip igmp snooping router-port-expire-time

This command configures the query timeout. Use the **no** form to restore the default.

Syntax

ip igmp snooping router-port-expire-time *seconds*
no ip igmp snooping router-port-expire-time

seconds - The time the switch waits after the previous querier stops before it considers the router port (i.e., the interface which had been receiving query packets) to have expired.
(Range: 300-500)

Default Setting

300 seconds

Command Mode

Global Configuration

Command Usage

The switch must use IGMPv2 for this command to take effect.

Example

The following shows how to configure the default timeout to 300 seconds:

```
Console(config)#ip igmp snooping router-port-expire-time 300
Console(config)#
```

Related Commands

ip igmp snooping version (4-157)

Static Multicast Routing Commands

Command	Function	Mode	Page
ip igmp snooping vlan mrouter	Adds a multicast router port	GC	4-163
show ip igmp snooping mrouter	Shows multicast router ports	PE	4-164

ip igmp snooping vlan mrouter

This command statically configures a multicast router port. Use the **no** form to remove the configuration.

Syntax

[**no**] **ip igmp snooping vlan** *vlan-id* **mrouter** *interface*

- *vlan-id* - VLAN ID (Range: 1-4093)
- *interface*
  - **ethernet** *unit*/*port*
    - *unit* - This is device 1.
    - *port* - Port number.
  - **port-channel** *channel-id* (Value: 1)

Default Setting

No static multicast router ports are configured.

Command Mode

Global Configuration

Command Usage

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/switch connected over the network to an interface (port or trunk) on your router, you can manually configure that interface to join all the current multicast groups.

Example

The following shows how to configure port 11 as a multicast router port within VLAN 1:

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11
Console(config)#
```

show ip igmp snooping mrouter

This command displays information on statically configured and dynamically learned multicast router ports.

Syntax

show ip igmp snooping mrouter [**vlan** *vlan-id*]

vlan-id - VLAN ID (Range: 1-4093)

Default Setting

Displays multicast router ports for all configured VLANs.

Command Mode

Privileged Exec

Command Usage

Multicast router port types displayed include Static or Dynamic.

Example

The following shows that port 11 in VLAN 1 is attached to a multicast router:

```
Console#show ip igmp snooping mrouter vlan 1
 VLAN M'cast Router Ports Type
 ---- ------------------- -------
    1            Eth 1/11  Static
    2            Eth 1/12  Dynamic
Console#
```

IP Interface Commands

There are no IP addresses assigned to this switch by default. You must manually configure a new address to manage the switch over your network or to connect the switch to existing IP subnets. You may also need to a establish a default gateway between this device and management stations or other devices that exist on another network segment.

Basic IP Configuration

Command	Function	Mode	Page
ip address	Sets the IP address for the current interface	IC	4-165
ip default-gateway	Defines the default gateway through which this switch can reach other subnetworks	GC	4-166
show ip interface	Displays the IP settings for this device	PE	4-166
show ip redirects	Displays the default gateway configured for this device	PE	4-167
ping	Sends ICMP echo request packets to another node on the network	NE, PE	4-167

ip address

This command sets the IP address for the currently selected VLAN interface. Use the **no** form to restore the default IP address.

Syntax

ip address {*ip-address netmask* | **bootp** | **dhcp**}
no ip address

- *ip-address* - IP address
- *netmask* - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **bootp** - Obtains IP address from BOOTP.
- **dhcp** - Obtains IP address from DHCP.

Default Setting

IP address: 0.0.0.0
Netmask: 255.0.0.0

Command Mode

Interface Configuration (VLAN)

Command Usage

- You must assign an IP address to this device to gain management access over the network or to connect the switch to existing IP subnets. You can manually configure a specific IP address, or direct the device to obtain an address from a BOOTP or DHCP server. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the configuration program.
- If you select the **bootp** or **dhcp** option, IP is enabled but will not function until a BOOTP or DHCP reply has been received. Requests will be broadcast periodically by this device in an effort to learn its IP address. (BOOTP and DHCP values can include the IP address, default gateway, and subnet mask).
- You can start broadcasting BOOTP or DHCP requests by entering an **ip dhcp restart client** command, or by rebooting the switch.

Note: Before you can change the IP address, you must first clear the current address with the **no** form of this command.

Example

In the following example, the device is assigned an address in VLAN 1.

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#
```

Related Commands

ip dhcp restart client (4-85)

ip default-gateway

This command establishes a static route between this switch and devices that exist on another network segment. Use the **no** form to remove the static route.

Syntax

ip default-gateway *gateway*
no ip default-gateway

gateway - IP address of the default gateway

Default Setting

No static route is established.

Command Mode

Global Configuration

Command Usage

A gateway must be defined if the management station is located in a different IP segment.

Example

The following example defines a default gateway for this device:

```
Console(config)#ip default-gateway 10.1.1.254
Console(config)#
```

Related Commands

show ip redirects (4-167)

show ip interface

This command displays the settings of an IP interface.

Default Setting

All interfaces

Command Mode

Privileged Exec

Example

```
Console#show ip interface
 IP address and netmask: 192.168.1.54 255.255.255.0 on VLAN 1,
 and address mode: User specified.
Console#
```

Related Commands

show ip redirects (4-167)

show ip redirects

This command shows the default gateway configured for this device.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show ip redirects
ip default gateway 10.1.0.254
Console#
```

Related Commands

ip default-gateway (4-166)

ping

This command sends ICMP echo request packets to another node on the network.

Syntax

ping *host* [**count *count***][**size *size***]

- *host* - IP address or IP alias of the host.
- *count* - Number of packets to send. (Range: 1-16, default: 5)
- *size* - Number of bytes in a packet. (Range: 32-512, default: 32)
  The actual packet size will be eight bytes larger than the size specified because the switch adds header information.

Default Setting

This command has no default for the host.

Command Mode

Normal Exec, Privileged Exec

Command Usage

- Use the ping command to see if another site on the network can be reached.
- Following are some results of the **ping** command:
- *Normal response* - The normal response occurs in one to ten seconds, depending on network traffic.
- *Destination does not respond* - If the host does not respond, a “timeout” appears in ten seconds.
- *Destination unreachable* - The gateway for this destination indicates that the destination is unreachable.
- *Network or host unreachable* - The gateway found no corresponding entry in the route table.
- Press <Esc> to stop pinging.

Example

```
Console#ping 10.1.0.9
Type ESC to abort.
PING to 10.1.0.9, by 5 32-byte payload ICMP packets, timeout is 5 seconds
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 0 ms
Ping statistics for 10.1.0.9:
 5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
 Minimum = 0 ms, Maximum = 10 ms, Average = 8 ms
Console#
```

Related Commands

interface (4-86)

Appendix A: Software Specifications

Software Features

Authentication
  Local, RADIUS, TACACS, Port (802.1x), HTTPS, SSH, Port Security

DHCP Client

Port Configuration
  1000BASE-T: 10/100/1000 Mbps, half/full duplex
  1000BASE-SX/LX: 1000 Mbps, full duplex

Flow Control
  Full Duplex: IEEE 802.3x
  Half Duplex: Back pressure

Broadcast Storm Control
  Traffic throttled above a critical threshold

Port Mirroring
  Multiple source ports, one destination port

Rate Limits
  Input Limit
  Output limit
  Range (configured per port)

Port Trunking
  Static trunks (Cisco EtherChannel compliant)
  Dynamic trunks (Link Aggregation Control Protocol)

Spanning Tree Protocol
  Spanning Tree Protocol (STP, IEEE 802.1D)
  Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w)

VLAN Support
  Up to 255 groups; port-based, protocol-based, or tagged (802.1Q),

Class of Service
  Supports four levels of priority and Weighted Round Robin Queueing
  (which can be configured by VLAN tag or port),
  Layer 3/4 priority mapping: IP Precedence, IP DSCP

Multicast Filtering
  IGMP Snooping (Layer 2)

Additional Features
  BOOTP client
  CIDR (Classless Inter-Domain Routing)
  SNTP (Simple Network Time Protocol)
  SNMP (Simple Network Management Protocol)
  RMON (Remote Monitoring, groups 1,2,3,9)
  SMTP Email Alerts

Management Features

In-Band Management
Telnet, Web-based HTTP or HTTPS, SNMP manager, or Secure Shell

Out-of-Band Management
RS-232 DB-9 console port

Software Loading
TFTP in-band or XModem out-of-band

SNMP
Management access via MIB database
Trap management to specified hosts

RMON
Groups 1, 2, 3, 9 (Statistics, History, Alarm, Event)

Standards

IEEE 802.3 Ethernet,
IEEE 802.3u Fast Ethernet
IEEE 802.3x Full-duplex flow control (ISO/IEC 8802-3)
IEEE 802.3z Gigabit Ethernet,
IEEE 802.3ab 1000BASE-T
IEEE 802.3ac VLAN tagging
IEEE 802.1Q VLAN
IEEE 802.1v Protocol-based VLANs
IEEE 802.3ad Link Aggregation Control Protocol
IEEE 802.1D Spanning Tree Protocol and traffic priorities
IEEE 802.1p Priority tags
IEEE 802.1w Rapid Spanning Tree Protocol
IEEE 802.1x Port Authentication
ARP (RFC 826)
DHCP (RFC 1541)
HTTPS
ICMP (RFC 792)
IGMP (RFC 1112)
IGMPv2 (RFC 2236)
RADIUS+ (RFC 2618)
RMON (RFC 1757 groups 1,2,3,9)
SNTP (RFC 2030)
SNMP (RFC 1157)
SNMPv2 (RFC 1907)
SSH (Version 1.5)

Management Information Bases

Bridge MIB (RFC 1493)
Entity MIB (RFC 2737)
Ethernet MIB (RFC 2665)
Ether-like MIB (RFC 1643)
Extended Bridge MIB (RFC 2674)
Extensible SNMP Agents MIB (RFC 2742)
Forwarding Table MIB (RFC 2096)
IGMP MIB (RFC 2933)
Interface Group MIB (RFC 2233)
Interfaces Evolution MIB (RFC 2863)
IP Multicasting related MIBs
MAU MIB (RFC 2668)
MIB II (RFC 1213)
Port Access Entity MIB (IEEE 802.1x)
Private MIB
Quality of Service MIB
RADIUS Authentication Client MIB (RFC 2618)
RMON MIB (RFC 2819)
RMON II Probe Configuration Group (RFC 2021, partial implementation)
TACACS+ Authentication Client MIB
TCP MIB (RFC 2013)
Trap (RFC 1215)
UDP MIB (RFC 2012)

Appendix B: Troubleshooting

Troubleshooting Chart	
Symptom	**Action**
Cannot connect using Telnet, Web browser, or SNMP software	• Be sure you have configured the agent with a valid IP address, subnet mask and default gateway. • If you are trying to connect to the agent via the IP address for a tagged VLAN group, your management station must include the appropriate tag in its transmitted frames. • Check that you have a valid network connection to the switch and that the port you are using has not been disabled. • Check network cabling between the management station and the switch. • If you cannot connect using Telnet or SSH, you may have exceeded the maximum number of concurrent Telnet/SSH sessions permitted. Try connecting again at a later time.
Cannot access the on-board configuration program via a serial port connection	• Be sure you have set the terminal emulator program to VT100 compatible, 8 data bits, 1 stop bit, no parity, and the baud rate set to any of the following (9600, 19200, 38400, 57600, 115200 bps). • Check that the null-modem serial cable conforms to the pin-out connections provided in the Installation Guide.
Forgot or lost the password	• Contact your local distributor.

Glossary

Boot Protocol (BOOTP)

BOOTP is used to provide bootup information for network devices, including IP address information, the address of the TFTP server that contains the devices system files, and the name of the boot file.

Class of Service (CoS)

CoS is supported by prioritizing packets based on the required level of service, and then placing them in the appropriate output queue. Data is transmitted from the queues using weighted round-robin service to enforce priority service and prevent blockage of lower-level queues. Priority may be set according to the port default, the packet's priority bit (in the VLAN tag), TCP/UDP port number, IP Precedence bit, or DSCP priority bit.

Customer Premises Equipment (CPE)

Terminating equipment, such as terminals, phones, routers and routers, supplied by the phone company, installed at customer sites, and connected to the phone company network.

Differentiated Services Code Point Service (DSCP)

DSCP uses a six-bit tag to provide for up to 64 different forwarding behaviors. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP bits are mapped to the Class of Service categories, and then into the output queues.

Domain Name Service (DNS)

A system used for translating host names for network nodes into IP addresses.

Dynamic Host Control Protocol (DHCP)

Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

Extensible Authentication Protocol over LAN (EAPOL)

EAPOL is a client authentication protocol used by this switch to verify the network access rights for any device that is plugged into the switch. A user name and password is requested by the switch, and then passed to an authentication server (e.g., RADIUS) for verification. EAPOL is implemented as part of the IEEE 802.1x Port Authentication standard.

GARP VLAN Registration Protocol (GVRP)

Defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports along the Spanning Tree so that VLANs defined in each switch can work automatically over a Spanning Tree network.

Generic Attribute Registration Protocol (GARP)

GARP is a protocol that can be used by endstations and switches to register and propagate multicast group membership information in a switched environment so that multicast data frames are propagated only to those parts of a switched LAN containing registered endstations. Formerly called Group Address Registration Protocol.

Generic Multicast Registration Protocol (GMRP)

GMRP allows network devices to register end stations with multicast groups. GMRP requires that any participating network devices or end stations comply with the IEEE 802.1p standard.

Group Attribute Registration Protocol (GARP)

See Generic Attribute Registration Protocol.

IEEE 802.1D

Specifies a general method for the operation of MAC bridges, including the Spanning Tree Protocol.

IEEE 802.1Q

VLAN Tagging—Defines Ethernet frame tags which carry VLAN information. It allows switches to assign endstations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks.

IEEE 802.1p

An IEEE standard for providing quality of service (QoS) in Ethernet networks. The standard uses packet tags that define up to eight traffic classes and allows switches to transmit packets based on the tagged priority value.

IEEE 802.1s

An IEEE standard for the Multiple Spanning Tree Protocol (MSTP) which provides independent spanning trees for VLAN groups.

IEEE 802.1x

Port Authentication controls access to the switch ports by requiring users to first enter a user ID and password for authentication.

IEEE 802.3ac

Defines frame extensions for VLAN tagging.

IEEE 802.3x

Defines Ethernet frame start/stop requests and timers used for flow control on full-duplex links.

IGMP Snooping

Listening to IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to identify IP Multicast group members.

IGMP Query

On each subnetwork, one IGMP-capable device will act as the querier — that is, the device that asks all hosts to report on the IP multicast groups they wish to join or to which they already belong. The elected querier will be the device with the lowest IP address in the subnetwork.

Internet Group Management Protocol (IGMP)

A protocol through which hosts can register with their local router for multicast services. If there is more than one multicast switch/router on a given subnetwork, one of the devices is made the “querier” and assumes responsibility for keeping track of group membership.

In-Band Management

Management of the network from a station attached directly to the network.

IP Multicast Filtering

A process whereby this switch can pass multicast traffic along to participating hosts.

IP Precedence

The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The eight values are mapped one-to-one to the Class of Service categories by default, but may be configured differently to suit the requirements for specific network applications.

Layer 2

Data Link layer in the ISO 7-Layer Data Communications Protocol. This is related directly to the hardware interface for network devices and passes on traffic based on MAC addresses.

Link Aggregation

See Port Trunk.

Link Aggregation Control Protocol (LACP)

Allows ports to automatically negotiate a trunked link with LACP-configured ports on another device.

Management Information Base (MIB)

An acronym for Management Information Base. It is a set of database objects that contains information about a specific device.

Multicast Switching

A process whereby the switch filters incoming multicast frames for services for which no attached host has registered, or forwards them to all ports contained within the designated multicast VLAN group.

Network Time Protocol (NTP)

NTP provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical-master-slave configuration in order to synchronize local clocks within the subnet and to national time standards via wire or radio.

Out-of-Band Management

Management of the network from a station not attached to the network.

Port Authentication

See IEEE 802.1x.

Private Branch Exchange (PBX)

A telephone exchange local to a particular organisation who use, rather than provide, telephone services.

POTS

Plain Old Telephone Service.

Port Mirroring

A method whereby data on a target port is mirrored to a monitor port for troubleshooting with a logic analyzer or RMON probe. This allows data on the target port to be studied unobstructively.

Port Trunk

Defines a network link aggregation and trunking method which specifies how to create a single high-speed logical link that combines several lower-speed physical links.

Private VLANs

Private VLANs provide port-based security and isolation between ports within the assigned VLAN. Data traffic on downlink ports can only be forwarded to, and from, uplink ports.

Remote Authentication Dial-in User Service (RADIUS)

RADIUS is a logon authentication protocol that uses software running on a central server to control access to RADIUS-compliant devices on the network.

Remote Monitoring (RMON)

RMON provides comprehensive network monitoring capabilities. It eliminates the polling required in standard SNMP, and can set alarms on a variety of traffic conditions, including specific error types.

Rapid Spanning Tree Protocol (RSTP)

RSTP reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard.

Secure Shell (SSH)

A secure replacement for remote access functions, including Telnet. SSH can authenticate users with a cryptographic key, and encrypt data connections between management clients and the switch.

Simple Mail Transfer Protocol (SMTP)

A standard host-to-host mail transport protocol that operates over TCP, port 25.

Simple Network Management Protocol (SNMP)

The application protocol in the Internet suite of protocols which offers network management services.

Simple Network Time Protocol (SNTP)

SNTP allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server, or can be received via broadcasts sent by NTP servers.

Spanning Tree Protocol (STP)

A technology that checks your network for any loops. A loop can often occur in complicated or backup linked network systems. Spanning Tree detects and directs data along the shortest available path, maximizing the performance and efficiency of the network.

Terminal Access Controller Access Control System Plus (TACACS+)

TACACS+ is a logon authentication protocol that uses software running on a central server to control access to TACACS-compliant devices on the network.

Telnet

Defines a remote communication facility for interfacing to a terminal device over TCP/IP.

Transmission Control Protocol/Internet Protocol (TCP/IP)

Protocol suite that includes TCP as the primary transport protocol, and IP as the network layer protocol.

Trivial File Transfer Protocol (TFTP)

A TCP/IP protocol commonly used for software downloads.

User Datagram Protocol (UDP)

UDP provides a datagram mode for packet-switched communications. It uses IP as the underlying transport mechanism to provide access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.

VDSL

Very high data rate Digital Subscriber Line: A family of digital telecommunications protocols designed to allow high speed data communication at data rates from below 1 Mbps to 52.8 Mbps with corresponding maximum reach ranging from 4500 feet to 1000 feet of 24 gauge twisted pair cable over the existing copper telephone lines between end-users and telephone companies.

Virtual LAN (VLAN)

A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, and allows users to share information and resources as though located on the same LAN.

XModem

A protocol used to transfer files between devices. Data is grouped in 128-byte blocks and error-corrected.

Index

VS4512
VS4512DC
E112003-R01
150000041800A